

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-243536

(43)Date of publication of application : 07.09.1999

(51)Int.Cl.

H04N 7/16
H04H 1/00
H04L 9/08
H04L 9/32

BEST AVAILABLE COPY

(21)Application number : 10-228287

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 12.08.1998

(72)Inventor : AKIYAMA KOICHIRO
KAMIBAYASHI TATSU
TSUJIMOTO SHUICHI
ENDO NAOKI

(30)Priority

Priority number : 09366812

Priority date : 26.12.1997

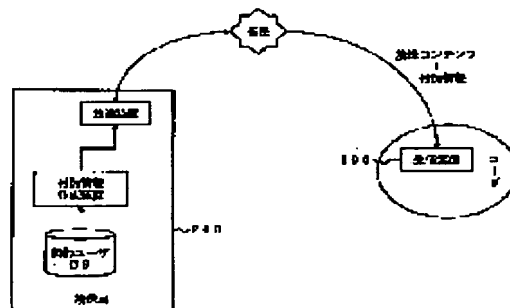
Priority country : JP

(54) BROADCAST RECEIVER AND CONTRACT MANAGEMENT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a broadcast receiver that realizes limited reception while keeping security of the same degree, even in the case that a broadcast band for transmission of information for limited reception is narrow and the number of subscribers have increased to more than expected.

SOLUTION: This system has a master key in common to plural broadcast receivers 100 and a respective receiver ID set specifically to each broadcast receiver. In the case of receiving encrypted reception contract information including at least contract information and a receiver ID corresponding to the contract information, the master key is used to sequentially decode the encrypted reception contract information. The contract information, corresponding to the receiver ID in matching with the receiver ID possessed by the broadcast receiver, is selected and acquired among the decoded reception contract information, and the system determines whether or not a channel key for decoding the encrypted information contents is fed to a decoding section in order to decode the encrypted contents information, based on the acquired contract information.



LEGAL STATUS

[Date of request for examination]

26.02.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

THIS PAGE LEFT BLANK

the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number] 3561154

[Date of registration] 04.06.2004

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

THIS PAGE LEFT BLANK

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-243536

(43) 公開日 平成11年(1999) 9月7日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 N 7/16

H 0 4 N 7/16

Z

H 0 4 H 1/00

H 0 4 H 1/00

F

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 A

9/32

6 7 1

審査請求 未請求 請求項の数21 O L (全 52 頁)

(21) 出願番号 特願平10-228287

(22) 出願日 平成10年(1998) 8月12日

(31) 優先権主張番号 特願平9-366812

(32) 優先日 平 9 (1997) 12月26日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 秋山 浩一郎

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(72) 発明者 上林 達

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(72) 発明者 辻本 修一

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(74) 代理人 弁理士 鈴江 武彦 (外6名)

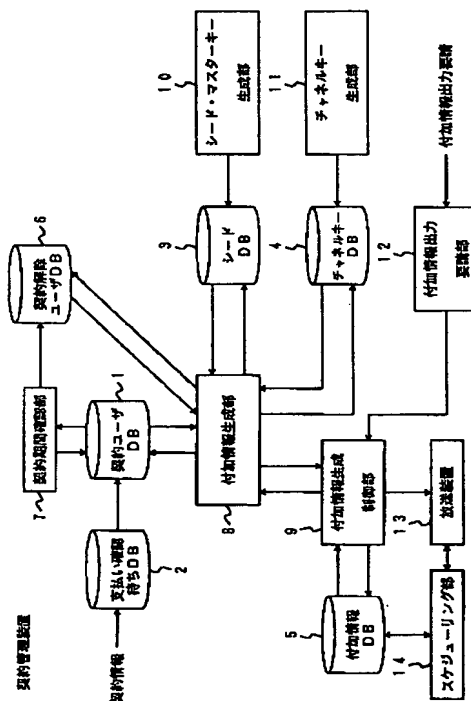
最終頁に続く

(54) 【発明の名称】 放送受信装置および契約管理装置

(57) 【要約】

【課題】 限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信が実現できる放送受信装置を提供する。

【解決手段】 複数の放送受信装置に共通のマスター鍵と本放送受信装置に固有に設定された受信装置 I D を持ち、少なくとも契約情報と該契約情報に対応した受信装置 I D を含む暗号化された受信契約情報を受信したとき、前記マスター鍵を用いて、該暗号化された受信契約情報を順次復号し、該復号された受信契約情報のうち、本放送受信装置の有する受信装置 I D に一致する受信装置 I D に対応付けられた契約情報を選択して取得し、その取得した契約情報に基づき、暗号化された情報コンテンツを復号するチャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るかを制御する。



【特許請求の範囲】

【請求項1】 暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき、放送配信される暗号化コンテンツ情報を復号する放送受信装置において、複数の放送受信装置に共通のマスター鍵と本放送受信装置に固有に設定された受信装置IDを持ち、少なくとも前記契約情報と該契約情報に対応した受信装置IDを含む暗号化された受信契約情報を受信したとき、前記マスター鍵を用いて、該暗号化された受信契約情報を順次復号し、

該復号された受信契約情報のうち、本放送受信装置の有する受信装置IDに一致する受信装置IDに対応付けられた契約情報を選択して取得し、

その取得した契約情報に基づき、暗号化された情報コンテンツを復号するチャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする放送受信装置。

【請求項2】 前記チャンネルキーは別途受信し、前記受信契約情報を受信しない限り、前記チャンネルキーは前記復号部に送られることがないように制御することを特徴とする請求項1記載の放送受信装置。

【請求項3】 暗号化された前記チャンネルキーを別途受信し、この暗号化されたチャンネルキーを復号するチャンネルキー復号鍵を含む前記受信契約情報を受信しない限り、前記チャンネルキーが復号されないよう制御することを特徴とする請求項1記載の放送受信装置。

【請求項4】 前記チャンネルキーの一部は別途受信され、前記チャンネルキーの他の一部を含む前記受信契約情報を受信しない限り、前記チャンネルキーが得られないように制御することを特徴とする請求項1記載の放送受信装置。

【請求項5】 前記チャンネルキーは、前記受信契約情報に含まれて受信され、前記受信契約情報を受信しない限り、前記チャンネルキーが得られないものであることを特徴とする請求項1記載の放送受信装置。

【請求項6】 暗号化されたコンテンツ情報を含む通常放送波を受信する第1の受信手段と、前記暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段と、を具備し、

前記マスター鍵を用いて、前記第1もしくは第2の受信手段で受信した暗号化されたチャンネルキーを復号してチャンネルキーを取得するとともに、前記第2の受信手段で受信した暗号化された受信契約情報を復号して前記契約情報を取得し、

その取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする請求項1記載の放送受信装置。

【請求項7】 暗号化されたコンテンツ情報を含む通常

放送波を受信する第1の受信手段と、

前記暗号化されたチャンネルキーを復号するためのチャンネルキー復号鍵を含む暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段と、

を具備し、

前記マスター鍵を用いて、前記第2の受信手段で受信した暗号化された受信契約情報を復号して前記チャンネルキー復号鍵を取得し、

その取得したチャンネルキー復号鍵を用いて、前記第1もしくは第2の受信手段で受信した暗号化チャンネルキーを復号することによってチャンネルキーを取得し、

前記取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする請求項1記載の放送受信装置。

【請求項8】 暗号化された放送コンテンツ情報と前記チャンネルキーの一部を含む通常放送波を受信する第1の受信手段と、

前記チャンネルキーの他の一部を含む暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段を具備し、

前記マスター鍵を用いて、前記第2の受信手段で受信した暗号化された受信契約情報を復号して前記チャンネルキーの他の一部と前記契約情報を取得し、

前記第1の受信手段で受信したチャンネルキーの一部と前記取得したチャンネルキーの他の一部とからチャンネルキーを再生し、

前記取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする請求項1記載の放送受信装置。

【請求項9】 暗号化されたコンテンツ情報を含む通常放送波を受信する第1の受信手段と、

前記チャンネルキーを含む暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段と、

を具備し、

前記マスター鍵を用いて、前記第2の受信手段で受信した暗号化された受信契約情報を復号して該受信契約情報に含まれる契約情報とチャンネルキーを取得し、

その取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報の復号部に送るか否か制御することを特徴とする請求項1記載の放送受信装置。

【請求項10】 暗号化されたコンテンツ情報を復号するための内容の正確性が要求される必須情報の誤受信検出のために、それぞれの必須情報に認証子が付加されたデータを受信し、前記認証子とそれが付加された必須情報とを照合し、照合に失敗した場合は当該必須情報を無効にすることを特徴とする請求項1記載の放送受信装置。

【請求項11】 前記受信契約情報に含まれるデジタル

署名を検証し、検証により正当性の確認されたデジタル署名を持つ受信契約情報に含まれる契約情報のみを受理することを特徴とする請求項 1 記載の放送受信装置。

【請求項 12】 内部データをテスト出力するためのテスト制御部を具備し、

このテスト制御部は、前記受信契約情報に付加されたテスト用である旨の識別子を確認することにより、あるいは、該受信契約情報に付加されたデジタル署名の正当性を確認することにより、前記内部データをテスト出力するか否かを制御することを特徴とする請求項 1 記載の放送受信装置。

【請求項 13】 暗号化された受信契約情報を記録したカード型記録媒体から該暗号化された受信契約情報を読み出して本放送受信装置に受信させるカードリーダーを具備したことを特徴とする請求項 1 記載の放送受信装置。

【請求項 14】 暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャンネルキーは暗号化されたコンテンツ情報を復号するための復号部に送られることがないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、

少なくとも放送受信装置毎個別に設定された受信装置 ID と該受信装置 ID に対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、

前記チャンネルキーは前記受信契約情報とは別途配信することを特徴とする契約管理装置。

【請求項 15】 暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するための暗号化されたチャンネルキーが復号されないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置 ID と該受信装置 ID に対応した契約情報と前記暗号化されたチャンネルキーを復号するためのチャンネルキー復号鍵とを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする契約管理装置。

【請求項 16】 暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャンネルキーが得られないように制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置 ID と、該受信装置 ID に対応した契約情報として前記チャンネルキーの一部を含むものとを包含する受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して

送信し、

前記チャンネルキーの他の一部を別途送信することを特徴とする契約管理装置。

【請求項 17】 暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャンネルキーが得られないように、複数の放送受信装置を管理する契約管理装置であって、

少なくとも放送受信装置毎個別に設定された受信装置 ID と該受信装置 ID に対応した契約情報と前記チャンネルキーとを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする契約管理装置。

【請求項 18】 カード型記録媒体に前記暗号化された受信契約情報を記録する記録手段を具備したことを特徴とする請求項 14～請求項 17 のいずれか 1 つに記載の契約管理装置。

【請求項 19】 契約に変化の生じた契約者の受信契約情報を選択的に送信することを特徴とする請求項 14～請求項 17 のいずれか 1 つに記載の契約管理装置。

【請求項 20】 前記受信契約情報に含まれる情報の種別に応じた識別子に基づき、該受信契約情報に対する処理形態を切り替えることを特徴とする請求項 1～請求項 13 のいずれか 1 つに記載の放送受信装置。

【請求項 21】 前記受信契約情報を送信すべき契約者の数に応じて、受信契約情報の送信形態を切り替えることを特徴とする請求項 14～請求項 17 のいずれか 1 つに記載の契約管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、たとえば、契約内容（期間、視聴チャンネル）に応じて放送配信されるコンテンツを復号する有料放送サービスのための契約管理装置およびこの契約管理装置にてコンテンツの復号が制御されるコンテンツの受信装置に関する。

【0002】

【従来の技術】ディジタル放送は、通信衛星（CS）に始まって、ケーブル TV、地上放送へとディジタル化が進むにつれ、いっそうのサービスの充実が期待されており、これからの放送サービスの主役をつとめていくものと思われる。

【0003】ディジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャンネル数の大幅な増加が可能となったことである。さらに、高度な誤り訂正技術が適用されるため、高品質で均質なサービスの提供が可能となる。

【0004】放送のディジタル化により、多様な情報形態（映像、音声、文字、データ等）によるマルチメディアサービスの提供が可能となり、そのようなサービスを

提供するためのシステムも続々登場してきている。

【0005】このようなシステムで、契約内容に基づいてスクランブルを解く、あるいは復号する有料放送サービスを提供する際、契約期間に即した顧客管理が行えなければいけない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャンネルの番組の視聴を可能とするというものである。

【0006】また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する上からも正当な視聴者のみに（契約チャンネル、契約期間に即して）しかも確実に提供する必要がある。

【0007】この意味で、従来は、放送受信装置毎にマスター鍵を用意し、受信契約している視聴者に対して受信契約しているチャンネルのワークキーのみをマスター鍵で暗号化して送っていた。ここでワークキーはチャンネル固有の鍵であり、暗号化されて送られてくる当該チャンネルのチャンネルキーを復号することができる。チャンネルキーはスクランブルされた放送コンテンツをデスクランブルするのに用いられる。

【0008】さらに、ワークキーは契約期間（通常1ヶ月）毎に設定され、その期間毎に放送局から送られて来る。このため契約期間毎各契約者に必要十分なワークキーを送らなくてはならない。だが逆に見ればワークキーが更新されることにより確実に契約期間が守られるという長所があった。しかし、このシステムを取る限り1ヶ月毎に全契約者に対してワークキーを放送波で送らなければならず、CS放送の契約者やチャンネルが増加傾向にある今日送信量の観点からはかなり厳しくなりつつある。

【0009】

【発明が解決しようとする課題】そこで、本発明は、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信が実現できる放送受信装置、放送受信装置と放送送信装置（契約管理装置）を用いた限定受信システムを構築することを目的としている。

【0010】

【課題を解決するための手段】（1）請求項1
暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき、放送配信される暗号化コンテンツ情報を復号する放送受信装置において、複数の放送受信装置に共通のマスター鍵と本放送受信装置に固有に設定された受信装置IDを持ち、少なくとも前記契約情報と該契約情報に対応した受信装置IDを含む暗号化された受信契約情報を受信したとき、前記マスター鍵を用いて、該暗号化された受信契約情報を順次復号し、該復号された受信契約情報のうち、本放送受信装置の有する受信装置IDに一致する受信装置IDに対応付けられた契約情報

を選択して取得し、その取得した契約情報に基づき、暗号化された情報コンテンツを復号するチャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否かを制御することを特徴とする。

【0011】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信が実現できる。例えば、契約期間に限って当該顧客のみに契約チャンネルのコンテンツの視聴が可能となるような限定受信が行える。

【0012】（2）請求項2：第2の実施形態（チャンネルキーは、受信契約情報とは別途に配布）
請求項1記載の放送受信装置において、前記チャンネルキーは別途受信し、前記受信契約情報を受信しない限り、前記チャンネルキーは前記復号部に送られることがないように制御することを特徴とする。

【0013】（3）請求項3：第3の実施形態（受信契約情報にチャンネルキー復号鍵が含まれる）
請求項1記載の放送受信装置において、暗号化された前記チャンネルキーを別途受信し、この暗号化されたチャンネルキーを復号するチャンネルキー復号鍵を含む前記受信契約情報を受信しない限り、前記チャンネルキーが復号されないよう制御することを特徴とする。

【0014】（4）請求項4：第1の実施形態（受信契約情報にチャンネルキーの一部が含まれる）
請求項1記載の放送受信装置において、前記チャンネルキーの一部は別途受信され、前記チャンネルキーの他の一部を含む前記受信契約情報を受信しない限り、前記チャンネルキーが得られないように制御することを特徴とする。

【0015】（5）請求項5：第4の実施形態（受信契約情報にチャンネルキーが含まれる）
請求項1記載の放送受信装置において、前記チャンネルキーは、前記受信契約情報に含まれて受信され、前記受信契約情報を受信しない限り、前記チャンネルキーが得られないものであることを特徴とする

（6）請求項6：第2の実施形態（チャンネルキーは、受信契約情報とは別途に配布）

請求項1記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第1の受信手段と、前記暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段と、を具備し、前記マスター鍵を用いて、前記第1もしくは第2の受信手段で受信した暗号化されたチャンネルキーを復号してチャンネルキーを取得するとともに、前記第2の受信手段で受信した暗号化された受信契約情報を復号して前記契約情報を取得し、その取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否かを制御することを特徴とする。

【0016】（7）請求項7：第3の実施形態（受信契約情報にチャンネルキー復号鍵が含まれる）

請求項 1 記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第 1 の受信手段と、前記暗号化されたチャンネルキーを復号するためのチャンネルキー復号鍵を含む暗号化された受信契約情報を含む契約放送波を受信する第 2 の受信手段と、を具備し、前記マスター鍵を用いて、前記第 2 の受信手段で受信した暗号化された受信契約情報を復号して前記チャンネルキー復号鍵を取得し、その取得したチャンネルキー復号鍵を用いて、前記第 1 もしくは第 2 の受信手段で受信した暗号化チャンネルキーを復号することによってチャンネルキーを取得し、前記取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【0017】(8) 請求項 8：第 1 の実施形態（受信契約情報にチャンネルキーの一部が含まれる）

請求項 1 記載の放送受信装置において、暗号化された放送コンテンツ情報と前記チャンネルキーの一部を含む通常放送波を受信する第 1 の受信手段と、前記チャンネルキーの他の一部を含む暗号化された受信契約情報を含む契約放送波を受信する第 2 の受信手段を具備し、前記マスター鍵を用いて、前記第 2 の受信手段で受信した暗号化された受信契約情報を復号して前記チャンネルキーの他の一部と前記契約情報を取得し、前記第 1 の受信手段で受信したチャンネルキーの一部と前記取得したチャンネルキーの他の一部とからチャンネルキーを再生し、前記取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【0018】(9) 請求項 9：第 4 の実施形態（受信契約情報にチャンネルキーが含まれる）

請求項 1 記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第 1 の受信手段と、前記チャンネルキーを含む暗号化された受信契約情報を含む契約放送波を受信する第 2 の受信手段と、を具備し、前記マスター鍵を用いて、前記第 2 の受信手段で受信した暗号化された受信契約情報を復号して該受信契約情報に含まれる契約情報とチャンネルキーを取得し、その取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報の復号部に送るか否か制御することを特徴とする。

(10) 請求項 1～請求項 9 の記載の放送受信装置において、チャンネルキー、マスター鍵の少なくとも一方が変更されることを特徴とする。

【0019】鍵情報に有効期間が定められていることにより、契約期間の管理（契約期間の開始、終了、継続等）が容易に行える。また、コンテンツの不正視聴防止等のセキュリティの向上が図れる。

(11) 請求項 1、請求項 3、請求項 7 記載の放送受信装置において、チャンネルキーおよびチャンネルキー復号鍵およびマスター鍵のうちの少なくとも 1 つが変更される

ことを特徴とする。

【0020】鍵情報に有効期間が定められていることにより、契約期間の管理（契約期間の開始、終了、継続等）が容易に行える。また、コンテンツの不正視聴防止等のセキュリティの向上が図れる。

(12) 請求項 1～請求項 9 の記載の放送受信装置において、チャンネルキー、マスター鍵の少なくとも一方が変更され、チャンネルキー、マスター鍵のそれぞれは、同時に最大 2 つの鍵を保持することを特徴とする。

(13) 請求項 1～請求項 9 の記載の放送受信装置において、チャンネルキー、マスター鍵の少なくとも一方が変更され、チャンネルキー、マスター鍵のそれぞれにおいて同時に最大 2 つの鍵を保持し、鍵変更の際には古い方を更新することを特徴とする。

(14) 請求項 1、請求項 3、請求項 7 記載の放送受信装置において、チャンネルキーおよびチャンネルキー復号鍵およびマスター鍵のうちの少なくとも一つが変更され、チャンネルキー、チャンネルキー復号鍵、マスター鍵のそれぞれは、同時に最大 2 つの鍵を保持することを特徴とする。

(15) 請求項 1、請求項 3、請求項 7 記載の放送受信装置において、チャンネルキーおよびチャンネルキー復号鍵およびマスター鍵のうちの少なくとも 1 つが変更され、チャンネルキー、チャンネルキー復号鍵、マスター鍵のそれぞれは、同時に最大 2 つの鍵を保持し、鍵変更の際には古い方を更新することを特徴とする。

(16) 請求項 1～請求項 9 の記載の放送受信装置において、チャンネルキーは、チャンネル毎に同時に最大 2 つ保持することを特徴とする。

【0021】チャンネルキーをチャンネル毎に最大 2 つ保持することにより、チャンネル切替時であっても（切替元にチャンネルの受信契約を行っていれば）、保持している当該チャンネルのチャンネルキーを暗号化されたコンテンツ情報の復号部に即時的に送ることでチャンネル切替の受信状態を良好にできる。

(17) 請求項 10

請求項 1 記載の放送受信装置において、暗号化されたコンテンツ情報を復号するための内容の正確性が要求される必須情報（例えば、チャンネルキー等の鍵情報、受信契約情報）の誤受信検出のために、それぞれの必須情報に認証子が付加されたデータを受信し、前記認証子とそれが付加された必須情報とを照合し、照合に失敗した場合は当該必須情報を無効にすることを特徴とする。

(18) 請求項 10 記載の放送受信装置において、暗号化された必須情報の認証子は、該必須情報を該必須情報で暗号化したもの、あるいは、その一部であることを特徴とする。

(19) 請求項 10 記載の放送受信装置において、暗号化された必須情報の認証子は、該必須情報を該必須情報で暗号化したもの、あるいは、前記暗号化された必須情

報を該必須情報で再暗号化したもの、あるいは、数回再暗号化した情報のうち全部あるいは一部であることを特徴とする。

(20) 請求項 10 記載の放送受信装置において、暗号化されていない必須情報（例えば、マスター鍵シード）の認証子は、該必須情報を必要があればブロック分割し、それぞれのブロックの情報を鍵として当該情報を暗号化したもの、あるいは、それをさらに圧縮したものをを用いることを特徴とする。

(21) 請求項 11

請求項 1 記載の放送受信装置において、前記受信契約情報に含まれるデジタル署名を検証し、検証により正当性の確認されたデジタル署名を持つ受信契約情報に含まれる契約情報のみを受理することを特徴とする。

(22) 請求項 11 記載の放送受信装置において、受信契約情報に当該放送受信装置に対する契約情報が含まれた時のみ、受信契約情報に含まれるデジタル署名を検証することを特徴とする。

(23) 請求項 11 記載の放送受信装置において、デジタル署名検証用の公開鍵を変更することを特徴とする。

(24) 請求項 12

請求項 1 記載の放送受信装置において、内部データ（復号された受信契約情報、放送受信装置内の受信装置 ID 格納部に格納されている受信装置 ID）をテスト出力するためのテスト制御部（スキャンバステスト用ラッチ部）を具備し、このテスト制御部は、前記受信契約情報に付加されたテスト用である旨の識別子を確認することにより、あるいは、該受信契約情報に付加されたデジタル署名の正当性を確認することにより、前記内部データをテスト出力するか否かを制御することを特徴とする。

(25) 請求項 12 記載の放送受信装置において、前記テスト制御部は、暗号化された内部データを出力することを特徴とする。

(26) 請求項 13

請求項 1 記載の放送受信装置において、暗号化された受信契約情報を記録したカード型記録媒体から該暗号化された受信契約情報を読み出して本放送受信装置に受信させるカードリーダを具備したことを特徴とする。

(27) 請求項 13 記載の放送受信装置において、前記カードリーダは、有効期間毎に複数の契約情報が記録された磁気カードから、前記複数の契約情報を読み出し、有効期間に応じてそれらの複数の契約情報を使い分けることを特徴とする。

(28) 契約管理装置

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき放送配信される暗号化コンテンツ情報を復号することにより該コンテンツ情報を受信する複数の放送受信装置を管理する契約管理装置において、少なくとも放送受信装置毎個別に設定された受信装置 ID と該

受信装置 ID に対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【0022】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(29) 請求項 14：第 2 の実施形態の契約管理装置

10 暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャンネルキーは暗号化されたコンテンツ情報を復号するための復号部に送られることがないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置 ID と該受信装置 ID に対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、前記チャンネルキーは前記受信契約情報とは別途配信することを特徴とする。

【0023】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(30) 請求項 15：第 3 の実施形態の契約管理装置

暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するための暗号化されたチャンネルキーが復号されないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置 ID と該受信装置 ID に対応した契約情報と前記暗号化されたチャンネルキーを復号するためのチャンネルキー復号鍵を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【0024】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(31) 請求項 16：第 1 の実施形態の契約管理装置

暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャンネルキーが得られないように制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別

に設定された受信装置 I D と、該受信装置 I D に対応した契約情報として前記チャンネルキーの一部を含むものとを包含する受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、前記チャンネルキーの他の一部を別途送信することを特徴とする。

【0025】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまう場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(32) 請求項 17：第 4 の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャンネルキーが得られないように、複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置 I D と該受信装置 I D に対応した契約情報と前記チャンネルキーとを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【0026】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまう場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(33) 請求項 14～15 記載の契約管理装置において、チャンネルキーおよびマスター鍵のうち少なくとも 1 つが予め定められた期間で変更されることを特徴とする。

(34) 請求項 14～17 記載の契約管理装置において、チャンネルキーおよびチャンネルキー復号鍵およびマスター鍵のうち少なくとも 1 つが予め定められた期間で変更されることを特徴とする。

(35) 請求項 14～17 記載の契約管理装置において、前受信契約情報に対する認証子を受信契約情報に含めて送信することを特徴とする。

(36) 請求項 14～17 記載の契約管理装置において、前記受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報に含まれる鍵情報で前記契約情報を暗号化したもの、もしくは、その一部を用いることを特徴とする。

(37) 請求項 14～17 記載の契約管理装置において、受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報に含まれる鍵情報を該鍵情報で暗号化したもの、前記暗号化された鍵情報を鍵情報で再暗号化したもの、もしくは数回再暗号化した情報のうち全部もしくは一部を用いることを特徴とする。

(38) 請求項 14～17 記載の契約管理装置において、受信契約情報に対する認証子を受信契約情報に含め

て送信し、該認証子として、受信契約情報を必要があればブロック分割し、それぞれのブロックの情報を鍵として当該情報を暗号化し、必要があれば圧縮したものを用的ことを特徴とする。

(39) 請求項 14～17 記載の契約管理装置において、受信契約情報に該受信契約情報に対するデジタル署名を付加して送信することを特徴とする。

10 (40) 請求項 14～17 記載の契約管理装置において、受信契約情報に該受信契約情報に対するデジタル署名を付加して送信し、デジタル署名検証用の公開鍵と作成用の秘密鍵のペアを生成する機構を具備し、一定期間で前記デジタル署名用の公開鍵と秘密鍵を変更すると共に、前記デジタル署名検証用の公開鍵を送信することを特徴とする。

(41) 請求項 18

請求項 14～17 に記載の契約管理装置において、カード型記録媒体に前記暗号化された受信契約情報を記録する記録手段を具備したことを特徴とする。

(42) 請求項 19

20 請求項 14～17 に記載の契約管理装置において、最近一定期間内に契約の変化の生じた（新規契約を含む）契約者の受信契約情報を選択的に送信することを特徴とする。

【0027】契約の種類（例えば、契約変更、新規契約など）と契約後の経過期間によって、契約情報の放送頻度を変更するようにしてもよい。

(42-1) 請求項 14～17 に記載の契約管理装置において、契約の変化の生じた（新規契約を含む）時期により、受信契約情報の送信頻度を変化させることを特徴とする。

(43) 請求項 20

請求項 1～請求項 13 記載の放送受信装置において、前記受信契約情報に含まれる情報の種別に応じた識別子（情報識別子）に基づき、該受信契約情報に対する処理形態を切り替えることを特徴とする。

(44) 請求項 21

請求項 14～17 記載の契約管理装置において、前記受信契約情報を送信すべき契約者の数に応じて、受信契約情報の送信形態を切り替えることを特徴とする。

40 【0028】

【発明の実施の形態】以下、本発明の実施形態について図面を参照して説明する。

【0029】（第 1 の実施形態）

1) 放送システムの概略

図 1 は、本発明の契約管理装置および放送受信装置を用いた放送システムの概略構成を示したもので、放送局 200 から衛星を利用して受信契約を行った各ユーザにコンテンツを提供するサービス形態の場合を示している。なお、図 1 では衛星放送の場合を例にとり説明するが、地上波にてコンテンツを提供するサービス形態の場合も

同様である。

【0030】図2は、図1に示した放送サービスへの加入・継続契約時、契約更新時、解約時、課金手続きの概略的に流れを示したものである。

【0031】図2に示すように、図1の放送サービスへの加入を希望するユーザは、加入手続きを代行する所定の代理店にて、視聴を希望するチャンネル、視聴期間等の契約内容に伴った所定の加入手続きを行う。代理店を介して、その契約内容が放送局側の契約ユーザデータベースに登録されると、その登録内容に従ったユーザへのサービス提供を開始する。このサービス提供に対してユーザが支払うべき料金を例えばクレジットカード、あるいは銀行を介しての支払うようにしてもよい。

【0032】ユーザへのサービス提供は、もっぱら、放送局側にある契約者データベースの登録内容に従ったものである。従って、加入時の契約内容の継続・更新、解約時等には、ユーザによる直接あるいは所定の代理店等を介してのその旨の通告を受けて、契約ユーザデータベースの登録内容を更新あるいは消去すればよい。なお、放送局は、加入料、受信料等の支払を確認した上で、当該ユーザへのサービス提供を開始あるいは継続するようにしてもよい。

【0033】2) 契約管理装置

(1) 図3は、本実施形態に係る契約管理装置の構成例を示したもので、図1の放送局200に設置されて用いられる。

【0034】放送局200では、チャンネル毎に予め定められたチャンネルキーKchによって暗号化したコンテンツ情報（「コンテンツ」Kch）、端末IDおよびチャンネルキーKch等を含む付加情報をマスターキーKmによって暗号化した付加情報（「付加情報」Km）を放送する。

【0035】付加情報は放送受信契約し、受信料を支払ったユーザのみに受信許可を与えるためのもので、各ユーザ宅に設置された受信装置は受信装置自身の持つマスターキーKmによって受信された暗号化付加情報（「付加情報」Km）を復号し、その中に含まれる端末IDと受信装置のもつ端末IDとを比較し、一致していた場合には、そこに含まれているチャンネルキーKchを受信装置の持つデータベースに格納し、暗号化されたコンテンツ情報（「コンテンツ」Kch）を復号するためにこれを用いる。

【0036】チャンネルキーKchは一定の期間（例えば1ヶ月）毎に変更され、契約期間が切れたユーザにはそれ以降の付加情報は送られず、対応するチャンネルキーKchが入手できないことから視聴できないことになる。

【0037】さらに、この方式の安全性を向上させるため、マスターキーKmを一定期間毎に更新する。これは受信装置と放送装置の両方に共通にある乱数発生器を用いて行ない、放送波ではその乱数発生器に乱数を発生さ

せる初期値（以下シードという）を受信装置に定期的に送る。これにより、たとえマスターキーKmが露見しても、一定期間しかそれが有効でないので、不正視聴を防止することが可能となる。また、復号鍵そのものを配信するのではなく、復号鍵を生成するために基となる情報を配信するので、セキュリティ性が高い。

【0038】さて、図3の契約管理装置は、付加情報の生成と、その生成された付加情報をマスターキーKmで暗号化して放送するためのものである。

10 【0039】まず、図7に示すフローチャートと図3を参照して、契約ユーザDB1の登録処理動作について説明する。図1の放送サービスへの加入を希望するユーザとの間で、放送契約がなされると、図3の契約管理装置に契約情報が入力され（ステップS1）、支払い確認待ちデータベース（DB）2に蓄えられる（ステップS2～ステップS3）。支払い確認待ちDB2において支払確認が済んだ項目から順次契約ユーザデータベース（DB）1に送られ、支払い確認待ちDB2からは消去される（ステップS2～ステップS4）。

20 【0040】契約ユーザDB1には、図4に示す形式でデータが蓄えられる。図4において受信端末IDは受信端末を特定するための情報であり、チャンネル番号は契約済みのチャンネルの番号である。契約期間は契約済みの期間（例えば1998年01月31日までなど）が予め定められた形式で記入されている。

【0041】契約期間は契約期間確認部7で一定のタイミングでその有効性を確認する。ここで無効とされた場合は契約解除ユーザデータベース（DB）6に当該契約情報を送り、契約ユーザDB1からは削除する。従って、契約期間の経過した（契約切れ）のユーザに関する情報は、契約ユーザDB1から消去されているため、付加情報は配信されない。

【0042】シードデータベース（DB）3は、シード・マスターキー生成部10が一定のタイミングで生成したマスターキー生成用のシードから生成されるマスターキーをそのシードID及び有効期限とともに、図5に示す形式で格納している。

【0043】チャンネルキーデータベース（DB）4は、チャンネルキー生成部11が一定のタイミングで生成したチャンネルキーをチャンネル番号、チャンネルキーIDやその有効期限とともに図6に示す形式で格納している。

【0044】次に、契約ユーザ毎に対応した付加情報を生成し、これを放送装置13を使って受信装置に送る手順を図8に示すフローチャートを参照して説明する。

【0045】付加情報生成制御部9は、付加情報生成部8に対し、付加情報生成の指示を送る（ステップS11）。この指示とは、例えば「1997年12月1日から1ヶ月間契約している契約ユーザの付加情報を送れ」なる内容のもので、予め定められた形式のビット列で表現されたものでもよい。このような指示が出されると付

加情報生成部8では契約ユーザDB1から1997年12月1日から少なくとも1ヶ月間契約しているユーザの情報を検索して、当該情報を読み込む(ステップS12→ステップS13)。契約ユーザDB1から読み込まれたユーザ情報(図4参照)から各ユーザの端末ID、チャンネル番号を得る(ステップS14)。

【0046】ここで、契約期間の最小単位は1ヶ月で、契約有効期限は1日にはじまり月末に終了するとし、チャンネルキーもこの契約最小期間に固有なものとする。すなわち、11月のチャンネルキーは12月のそれとは異なるものを用い、それぞれの月内では変更しないものとする。また、当然チャンネル番号が異なれば期間が同じでも違うチャンネルキーを使うものとする。

【0047】次に、付加情報生成部8は、チャンネルキーDB4から1997年12月1日から1997年12月31日に有効なチャンネルキーKchを検索して、当該チャンネルキーKchを読み込む(ステップS15)。また、シードDB3から1997年12月1日から1997年12月31日に有効なシードに対応したマスターキーKmを検索し、当該マスターキーKmを読み込む(ステップS16)。ここでもマスターキーの切り替えの最小単位は1ヶ月とする。ただマスターキーの場合その性格上必ずしも1ヶ月で切り替える必要はない。

【0048】以上によって得られた情報(各ユーザの端末ID、契約チャンネル番号、チャンネルキーKch)をもとに、付加情報生成部8では、図9(b)に示すような各ユーザ毎の付加情報を生成し、マスターキーKmで暗号化する(ステップS17)。ここで生成された各契約ユーザ毎の暗号化付加情報は順次付加情報生成制御部9、放送装置13に送られる。

【0049】放送装置は、暗号化付加情報を所定の周波数帯域の放送波に変換して各受信装置に向けて配信する(ステップS18)。

【0050】一方、各チャンネル番号に対応するチャンネルキーKchを用いて暗号化された暗号化コンテンツ情報(図9(a)参照)は、この付加情報とは別途(別の帯域で)送られ、受信装置ではその両方を受信するようになっている。

【0051】図10は、暗号化コンテンツ情報の生成および配信(放送)するための放送局200に設置されるコンテンツ情報の配信装置の構成例を示したものである。なお、図10において、図3と同一部分には同一符号を付している。

【0052】各チャンネルのコンテンツ情報は、図10に示すように、コンテンツ情報データベース(DB)21に蓄積されている。暗号化部22は、コンテンツ情報DB21から各チャンネル番号に対応したコンテンツ情報を読み出すとともに、チャンネルキーDB4から先ほどの付加情報生成範囲で有効なチャンネル番号毎のチャンネルキーを読み出して、各チャンネルのコンテンツ情報を当該チャ

ネル番号のチャンネルキーKchで暗号化し、情報付加部23に送る。

【0053】マスターキーKmを一定期間毎に更新する場合、情報付加部23では、シードDB3から先ほどの付加情報生成範囲で有効なマスターキーシードあるいはシードIDを読み出し、それを放送装置13へ出力する。

【0054】放送装置13では、チャンネルキーで暗号化されたコンテンツ情報およびマスターキーシードあるいはシードIDを多重して、所定の周波数帯域の放送波に変換して各受信装置に向けて配信する。

【0055】ユーザ毎チャンネル毎の付加情報を個別に送るため大量の情報を配信する必要が生じ、一度に全ての情報を送れない場合は付加情報生成部8で生成された付加情報を一旦付加情報データベース(DB)5に蓄えておき、そこから配信する部分を取り出して放送配信し、配信が終了した後、該付加情報DB5から消去するとしてもよい。あるいは、付加情報生成制御部9が付加情報の生成をコントロールし、配信できる範囲のものだけを付加情報生成部8に指示してもよい。

【0056】また、1回の放送だけでは受信装置が(何らかの理由で)受信できないこともある。このため、付加情報は契約期間の前から(可能な限り)何度も頻繁に送る必要がある。しかしそれでも(長期間受信不能なところに受信装置が存在するなどの理由で)受信できない場合もあるであろう。この場合、ユーザは視聴できなくなるので、ユーザからのクレームという形で放送局側にフィードバックがかかる。その際は、付加情報出力要請部12に端末IDと該当チャンネル番号を含む付加情報出力要請信号を送り、付加情報出力要請部12は付加情報生成制御部9にそれを送り、付加情報生成制御部9では契約ユーザDB1を検索し、有効な契約を確認したら前述の手続きに従って暗号化した付加情報を生成し、放送する。

【0057】(2)なお、上記説明では、付加情報にチャンネルキーKchそのものを含む場合について説明したが、この場合に限らず、チャンネルキーKchを例えば上位数十ビットと残りの下位数十ビットとの2つのチャンネルサブキーH、Lに分割して、一方のチャンネルサブキーHのみを付加情報に乗せ、他方のチャンネルサブキーLをチャンネルサブキーKchにて暗号化されたコンテンツ情報に付加(あるいは多重)して配信するようにしてもよい。

【0058】この場合の契約管理装置の付加情報生成部8では、チャンネルキーDB4から付加情報の生成範囲で有効なチャンネルキーからチャンネルサブキーHを抽出して、ユーザの端末ID、契約チャンネル番号、チャンネルサブキーHをもとに、図11(b)に示すような各ユーザ毎の付加情報を生成し、マスターキーKmで暗号化する。

【0059】また、図10に示したコンテンツ情報の配信装置の情報付加部23では、さらに、チャンネルキーDB4から先ほどの付加情報生成範囲で有効なチャンネル番号毎のチャンネルキーからチャンネルサブキーLを抽出して、放送装置13へ出力する。放送装置13からは、図11(a)に示すように、チャンネルキーで暗号化されたコンテンツ情報、チャンネルサブキーL、さらに必要に応じてマスターキーシードあるいはシードIDが多重された所定の周波数帯域の放送波が各受信装置に向けて配信される。

【0060】(3) 付加情報として、図12に示すような各契約ユーザ固有の付加情報(端末付加情報)と、図13に示すようなチャンネル番号に対応したチャンネル付加情報とを用いる場合を考える。

【0061】図12に示すように端末付加情報は、端末ID及びチャンネル番号と、当該端末IDにて識別される受信装置との契約が有効/無効を示す情報とから構成されている。これは端末付加情報に記載された端末IDを自身の端末IDとして持つ受信装置の受信契約が、同じく端末付加情報の記載されたチャンネル番号のチャンネルで

有効か無効かを示すものである。

【0062】端末付加情報を考えるとき、受信装置は、当該チャンネルの受信契約が有効であるという端末付加情報(以下、有効の端末付加情報あるいはON信号と呼ぶ場合がある)が来たら、それ以降当該チャンネルを無効とする端末付加情報(以下、無効の端末付加情報あるいはOFF信号と呼ぶことがある)が来るまで当該チャンネルは有効とし、逆に当該チャンネルの無効の端末付加情報が来たら、それ以降当該チャンネルの有効の端末付加情報が来るまで当該チャンネルを無効にする。

【0063】端末付加情報はチャンネルキーを含まないので全体のサイズを半分以下に減らせる特徴がある。すなわち、チャンネルキーで暗号化されたコンテンツの解読を防ぐため、チャンネルキーを最低限でも56bit程度必要となる一方、チャンネルキー以外の端末IDやチャンネル番号等の情報は30bit程度でも十分である。従って、付加情報にチャンネルキーを含めた場合、付加情報全体に対するチャンネルキーの占める割合が大きくなってしまふ。しかし、付加情報からチャンネルキーを除くことにより、付加情報全体のサイズが半分以下になる。このため、前述の方式よりも小さな付加情報を送ることになるため、単位時間あたりに送れる付加情報の数が増える。そればかりか、各ユーザ宛にチャンネルキーの切替時に同期して、例えば、1ヶ月毎に個別にチャンネルキーを送る必要がなく、端末付加情報を配信するのは新規契約時と契約切れの時のみであるから配信する全体の付加情報の量は激減する。

【0064】実際、この場合、ユーザ個別に配信する端末付加情報は、放送受信を有効にする時と無効にする時に配信すれば良いだけなので通常の場合、極めて少なく

て済む。

【0065】図12に示したような端末付加情報を配信する契約管理装置の構成は、図3と同様で動作が異なる。すなわち、付加情報生成部8は、端末付加情報を作成する際、チャンネルキーDB4を検索せずに、契約ユーザDB1とシードDB3と契約解除ユーザDB6の情報を検索して端末付加情報を作成するようになっている。これは、チャンネルキーを端末付加情報に含める必要がない一方、契約解除をしたユーザに対しては端末付加情報を送らなければならないためである。

【0066】図3の契約管理装置の処理動作について説明する。

【0067】契約情報が入力されて契約ユーザDB1へ登録処理は、図7のフローチャートに従って実行される。

【0068】付加情報生成制御部9は、付加情報生成部8を介して予め定められたタイミングで契約ユーザDB1に登録されている新規契約ユーザの情報を検索する。付加情報生成部8では、検索された新規契約ユーザの情報から端末IDと契約チャンネル番号を抽出し、図12に示したような端末付加情報を作成する(この場合は契約を有効にするのであるから有効の端末付加情報を作成する)。

【0069】更に、付加情報生成部8は、シードDB3を検索して、現在有効なマスターキーを抽出する。このマスターキーを使って先に生成された端末付加情報を暗号化し、付加情報生成制御部9に送る。

【0070】付加情報生成制御部9では、これを放送装置13に送り、予め定められた帯域で放送する。

【0071】ここで、配信すべき端末付加情報が多すぎて一時に放送できないこともあるであろう。そのときは生成された暗号化された端末付加情報を付加情報DB5に一時的に蓄えるよう付加情報生成制御部9が制御することも可能である。

【0072】契約ユーザ側では、ユーザ自身の持つ受信装置にて、図12に示したような端末付加情報を受信すると、受信装置内部の復号ユニット(後述)にて、これを復号して契約が有効であるか否かが確認される。有効である旨が記述されていたときに、当該チャンネルのチャンネルキーを用いて、例えば付加情報とは別帯域で配信されてくる当該チャンネルのコンテンツ情報を復号して、ユーザは所望の番組を視聴することができるようになる。

【0073】契約期間確認部7は、予め定められたタイミングで契約ユーザDB1を検索し、契約切れのユーザを検索する。検索された契約切れのユーザに関する情報は、契約解除ユーザDB6に登録する。

【0074】契約切れのユーザに対しては、無効の端末付加情報を配信する必要がある。そこで、付加情報生成制御部9は、前述の有効の端末付加情報を配信するときと同様、まず、付加情報生成部8を介して予め定められ

たタイミングで契約ユーザ DB 1 に登録されている新規契約ユーザの情報を検索する。

【0075】付加情報生成部 8 では、検索された新規契約ユーザの情報から端末 ID と契約チャンネル番号を抽出し、図 12 に示したような端末付加情報を作成する（この場合は契約を無効にするのであるから無効の端末付加情報を作成する）。更に、付加情報生成部 8 は、シード DB 3 を検索して、現在有効なマスターキーを抽出する。このマスターキーを使って先に生成された端末付加情報を暗号化し、付加情報生成制御部 9 に送る。付加情報生成制御部 9 では、これを放送装置 13 に送り、予め定められた帯域で放送する。

【0076】ここで、無効の端末付加情報を配信する場合は、1 度放送するだけでは（何らかの原因で）受信装置が確実に受信できない場合もあり、例えば、1 度発信した情報を何ヶ月かに渡って定期的に流すようにする必要がある。さもないと当該受信装置は永久的に視聴可能な状態になってしまい、受信契約を管理しているとは言えない状態に陥る。このことは、有効の端末付加情報を送る場合でも同様だが、この場合はユーザからのクレームによって未受信が検出され、付加情報出力要請部 12 を用いて、当該未受信の有効の端末付加情報を配信することもできるので、無効の端末付加情報を配信する場合ほど長い間流し続けなくてもよい。

【0077】次に、コンテンツ情報を復号するためのチャンネルキーの配信について説明する。

【0078】今、チャンネルキーを 1 ヶ月に 1 度変更するとして、これを図 13 に示すようなフォーマットでチャンネル番号、必要に応じてチャンネルキー ID とともにチャンネル付加情報として生成し、その時点で有効なマスターキーにて暗号化する。この暗号化されたチャンネル付加情報を所定のタイミングで端末付加情報を送るのと同じ帯域で配信する。

【0079】配信時に、端末付加情報とチャンネル付加情報とを区別するための例えばビット情報を、端末付加情報とチャンネル付加情報との暗号化されていない部分に付けておけばよい。

【0080】受信装置側では、該ビット情報をチェックして、チャンネル付加情報である場合には、それを復号し、さらにチャンネル付加情報に含まれるチャンネル番号をチェックして、現在受信契約しているチャンネル番号であれば、該チャンネル付加情報に含まれるチャンネルキー ID およびチャンネルキーを格納する処理を行なう。

【0081】ここで、チャンネルキーを変更する場合、実際にチャンネルキーを変更する時点よりも前に、変更するチャンネルキーを配信するのが望ましい。これにより、受信装置側ではチャンネルキーの変更に伴うコンテンツ情報の復号が連続して行える。例えば、1998 年 1 月 1 日から切り替わるチャンネルキーのチャンネル付加情報は 1997 年 12 月 15 日から送るようすれば、16 日間の

間に受信装置が当該チャンネルキーのチャンネル付加情報を受信する可能性は極めて高くなり、それを受信装置の所定のデータベースに格納しておけば、1997 年 12 月 31 日から 1998 年 1 月 1 日の間のチャンネルキーの切替えがスムーズに行え、ユーザは、連続的に所望のチャンネルの番組を視聴することが可能となる。

【0082】一方、新規契約したユーザの受信装置には（今まで受信契約していなかったのであるから）当該チャンネルキーが格納されていない。このため新規契約ユーザは契約後すぐには視聴できないという問題がある。この問題を解決するためには、チャンネル付加情報を頻繁に配信する必要がある。しかし、図 13 に示したようなチャンネル付加情報は、各ユーザ個別のものではなく、チャンネル番号に対応したものである（すなわち、各ユーザに共通して配信すべき情報であるので）、各ユーザ個別に配信する必要のある図 9（b）に示したような付加情報の場合と比較して、配信量は少なくすむので、チャンネル付加情報を頻繁に送ることは十分に可能である。

【0083】なお、チャンネル付加情報の配信は、チャンネルキー変更直前（1997 年 12 月 31 日）と直後（1998 年 1 月 1 日）には普段より頻繁に送るようすると効果的である。何故ならば、これらの期間には確実に受信して欲しいからである。同様のことは受信契約の更新時期（新規受信契約開始の時期や契約切れの時期）にも言える。

【0084】前述の（1）の説明では、チャンネルキーの切り替えをもって、同時に契約の切り替え（契約切れ／継続契約）を意味していたので、チャンネルキーの切替時と契約切替時とを同じ時期にしていたが、有効／無効の端末付加情報を用いる場合は、必ずしも同じ時期にする必要がない。

【0085】このように、有効／無効の端末付加情報とチャンネル付加情報とを用いる場合、契約ユーザに配信すべき付加情報の内容を各ユーザ個別の情報とユーザ共通の情報とにわけ、契約切替時期には端末付加情報を頻繁に配信し、チャンネルキーの切替時期にはチャンネル付加情報を頻繁に配信すればよいので、配信量の分散が図れる。

【0086】（4）上記（3）の説明では、有効／無効の付加情報を配信することにより、受信装置のコンテンツ情報の復号の可否を制御（新規契約時と契約切れ時の受信端末への制御）するものであった。これと同様の操作を、例えば、図 9（b）に示す付加情報を用いても行うことができる。

【0087】すなわち、契約期間中は、付加情報生成部 8 は、図 9（b）に示すような端末 ID、チャンネルキー、チャンネル番号を含む付加情報を生成して各ユーザ宛に配信するが、例えば 1 ヶ月（チャンネルキーの有効期間であると同時に契約期間の最小単位でもある期間）毎

に、契約契約解除ユーザ DB 6 を検索して、契約の切れたユーザに対しては、チャンネルキーを含まない付加情報を生成して配信するようにする。当該受信装置では（有効なチャンネルキーを受け取ることがないので）、以後コンテンツ情報の復号はできない。このように、チャンネルキーを含まない付加情報は、当該ユーザの受信装置に対し契約切れの旨を通知するとともに、当該受信装置での視聴を不可能とするための制御信号でもある。

【0088】図 11（b）に示したようなチャンネルサブキー H を含む付加情報を用いる場合も同様で、契約期間中は、付加情報生成部 8 は、図 11（b）に示すような端末 ID、チャンネルサブキー H、チャンネル番号を含む付加情報を生成して各ユーザ宛に配信するが、例えば 1 ヶ月（チャンネルキーの有効期間であると同時に契約期間の最小単位でもある期間）毎に、契約契約解除ユーザ DB 6 を検索して、契約の切れたユーザに対しては、チャンネルサブキーを含まない付加情報を生成して配信するようにする。当該受信装置では（チャンネルキーを生成するために必要なチャンネルサブキーを入手できないので）、以後コンテンツ情報の復号はできない。このように、チャンネルサブキーを含まない付加情報は、当該ユーザの受信装置に対し契約切れの旨を通知するとともに、当該受信装置での視聴を不可能とするための制御信号でもある。

【0089】（5）次に、図 3 に示す契約管理装置のスケジューリング部 14 について説明する。

【0090】スケジューリング部 14 は、付加情報 DB 5 に格納された付加情報を配信する際、および、放送装置 13 にて付加情報を配信する際に、各ユーザ側の受信装置にて確実に付加情報が受信されるように配信制御を行うものである。

【0091】すなわち、例えば、受信契約後、契約変更時、契約解約時、チャンネルキー等の更新時には付加情報を頻繁に送る必要があり、そのための付加情報の配信スケジュールに従って、付加情報の配信制御を行うのが、スケジューリング部 14 である。

【0092】付加情報の配信スケジュールとして、視聴率の高い番組が放送される時間帯に頻繁に送ることも付加情報をユーザ側に確実に配信する上で有効な手段である。

【0093】3）受信装置

（1）図 14 は、本実施形態に係る受信装置 100 の構成例を示したもので、前述の図 3 に示したような放送局側に設置されている契約管理装置で生成された付加情報および図 10 に示したようなコンテンツ情報の配信装置から出力される放送波を受信するためのものである。

【0094】ここで図 14 に示した受信装置 100 にて受信される放送波には、次のような情報が含まれているものとする。

- ・ マスターキーシード
- ・ 【付加情報】 Km …付加情報をマスターキー Km

で暗号化したもの

- ・ チャンネルサブキー L
- ・ 【コンテンツ】 Kch …コンテンツ情報をチャンネルキー Kch で暗号化したもの

マスターキーシードは、図 14 の受信装置 100 のマスターキー生成部 504 がマスターキーを生成する元になるデータである。

【0095】チャンネルサブキー L は、付加情報に含まれるチャンネルサブキー H と合わせて、チャンネルキー Kch を生成するための情報である。

【0096】なお、チャンネルサブキー L を放送波に多重化して配信しない場合もある。この場合、チャンネルキー Kch = チャンネルサブキー H となる。

【0097】付加情報は、次のような情報が含まれているものとする。

- ・ 端末 ID …受信装置の識別情報
- ・ チャンネル番号（複数も可）
- ・ チャンネルサブキー H

端末 ID にて識別される受信装置との間で契約されているチャンネルが 1 つのみの場合は、チャンネル番号を必ずしも含む必要はない。また、チャンネルサブキー H が含まれないことがある。

【0098】付加情報にチャンネルサブキー H が含まれる場合、当該付加情報は、当該端末 ID にて識別される受信装置が当該チャンネルを視聴する事を可能にする、いわゆる ON 信号である。

【0099】一方、付加情報にチャンネルサブキー H が含まれない場合、当該付加情報は、当該端末 ID にて識別される受信装置が当該チャンネルを使用することを禁止する、いわゆる OFF 信号となる。

【0100】前述の契約管理装置にて生成されて配信された付加情報を受信した図 14 の受信装置における契約管理のメカニズムの概要を述べる。

【0101】付加情報がチャンネルサブキー H を含む場合、復号ユニット 110 は、付加情報から抽出されたチャンネルサブキー H をチャンネルサブキー格納部 508 に格納する。従って、チャンネルデコード 509 は、チャンネルサブキー格納部 508 からチャンネルサブキー H を取得し、放送波に多重化して配信されるチャンネルサブキー L と合わせて、チャンネルキー Kch を生成することができる。そして、生成したチャンネルキー Kch を用いて、当該チャンネルのコンテンツ情報を正しく復号することができる。

【0102】付加情報に含まれる端末 ID と、受信装置に予め与えられている ID とが一致しない場合、復号ユニット 110 はチャンネルサブキー H をチャンネルサブキー格納部 508 に格納しない。

【0103】放送局 200 の契約管理装置は、契約済みの受信装置の ID とその際契約された視聴チャンネルの番号および当該チャンネルのチャンネルサブキー H を含む付加

情報を放送波に多重化して放送することによって、当該契約受信装置のみに、契約チャンネルの視聴を開始させることができる。

【0104】付加情報がチャンネルサブキーHを含まない場合、復号ユニット110は、チャンネルサブキー格納部508に対してチャンネルサブキーHの消去指示を出力する。当該チャンネルのコンテンツ情報はチャンネルキーKchによって暗号化されている。チャンネルデコーダ509は、チャンネルサブキーHを取得できず、従って、コンテンツ情報に多重化して配信されるチャンネルサブキーLと合わせて、チャンネルキーKchを生成することができない。すなわち、当該チャンネルのコンテンツ情報を復号することができないため再生が行われない。

【0105】放送局200の契約管理装置は、解約受信装置のIDと解約チャンネル番号を含み、かつチャンネルサブキーHを含まない付加情報を、放送波に多重化して放送する。これによって、当該解約受信装置のみに、契約チャンネルの視聴を禁止（すなわち、解約）することができる。

【0106】次に、図14の受信装置の処理動作を図15～図18に示すフローチャートを参照して、より詳細に説明する。

【0107】まず、受信部501が放送波を受信すると、A/D変換部502がデジタル信号に変換するとともに、当該信号中に含まれる情報をバケット化してフィルタ503に出力する（ステップS101～ステップS102）。

【0108】各バケットは、フラグ情報を有し、このフラグ情報にて当該バケットがマスターキーシードを含むバケットか、付加情報を含むバケットか、コンテンツ情報を含むバケットかを識別することができる。さらに、マスターキーシード、付加情報の最後のバケットには、終了フラグが記録されている。

【0109】フィルタ503は、マスターキーシード、付加情報それぞれのために、十分な大きさのバッファを有している。

【0110】入力されたバケットのフラグから、当該バケットにマスターキーシードが含まれていると判断した場合は、マスターキーシード用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでにマスターキーシード用バッファに格納されたバケットをマスターキー生成部504に転送する（ステップS103～ステップS106）。

【0111】入力されたバケットのフラグから、当該バケットに付加情報が含まれていると判断した場合は、付加情報用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでに付加情報用バッファに格納されたバケットを判定部507に転送する（ステップS107～ステップS

110）。

【0112】入力されたバケットのフラグから、当該バケットにコンテンツ情報、チャンネルサブキーLが含まれていると判断した場合は、当該バケットをチャンネルデコーダ509に転送する（ステップS111）。

【0113】マスターキー生成部504では、図16のフローチャートに示すように、フィルタ503から転送されてきたバケットからマスターキーシードを抽出し、マスターキーを生成し、その生成されたマスターキーをマスターキー格納部505に格納する（ステップS121～ステップS123）。

【0114】判定部507では、図17のフローチャートに示すように、フィルタ503からバケットが転送されてきたら、まず、マスターキー格納部505からマスターキーKmを読み込み、当該バケットから抽出された付加情報をマスターキーKmを用いて復号する（ステップS131～ステップS133）。

【0115】付加情報には必ず端末IDが含まれ、さらにチャンネル番号とチャンネルサブキーHとが含まれている場合もある。

【0116】判定部507は、付加情報から端末IDを抽出し、ID格納部506に予め格納されている自身の端末IDとを比較し、一致していたときに限り、後続の処理を実行する。不一致のときは、処理を中止する（ステップS134）。

【0117】付加情報に含まれていた端末IDと自身の端末IDとが一致したとき、次に、付加情報にチャンネルサブキーHが含まれているか否かチェックし（ステップS135）、チャンネルサブキーHが含まれているときは、それをチャンネルサブキー格納部508に格納する（ステップS136）。付加情報にチャンネルサブキーHが含まれていないときは、当該付加情報は、OFF信号であると判断できるので、チャンネルサブキー格納部508に既に格納されているチャンネルサブキーHを消去する（ステップS137）。

【0118】チャンネルデコーダ509では、図18のフローチャートに示すように、フィルタ503から転送されてきたバケットからチャンネルサブキーLを抽出したら（ステップS141～ステップS142）、チャンネルサブキー格納部508からチャンネルサブキーHを読み出して（ステップS143）、チャンネルキーKchを生成する（ステップS144）。ステップS109で、チャンネルサブキー格納部508のチャンネルサブキーHが消去されている場合、処理を終了する。

【0119】チャンネルサブキーHとLからチャンネルキーKchを生成するアルゴリズムは、予めチャンネルデコーダ509に格納されている。

【0120】さて、チャンネルデコーダ509は、チャンネルキーkchを生成すると、それをを用いてフィルタ503から転送されてきたバケットから抽出される暗号化コ

ンテンツ情報を復号し（ステップS145）、復号されたコンテンツ情報を順次、D/A変換部510に出力する（ステップS146）。

【0121】D/A変換部510では、チャンネルデコーダ509から送られてくるコンテンツ情報をアナログ信号に変換し（ステップS147）、再生部511にてアナログ信号の再生を行う（ステップS148）。

【0122】暗号の解読による不正な視聴を防止する観点から、暗号のキーは定期的に更新することが望ましい。例えば、放送に多重化して配信されるチャンネルサブキーLを変更することで、チャンネルキーKchを容易に変更することができる。勿論、この場合、チャンネルのコンテンツ情報は新しいチャンネルキーKchによって復号可能である様に暗号化されていなければならない。なお、チャンネルサブキーLを放送波に多重化して配信しない場合もある。この場合、チャンネルキーKch=チャンネルサブキーHとなる。

【0123】ところで、受信装置100は、視聴許可の付加情報を受信すると、視聴禁止の付加情報を受信するまで、契約チャンネルの番組視聴が可能である。ユーザがチャンネルの番組視聴契約を解除したにも係わらず、視聴禁止の付加情報を受信しないケースも考えられる。例えば、受信装置の電源が一定期間切断された様な場合である。従って、視聴禁止の付加情報（OFF信号）を解約後ある程度期間に渡って繰り返し放送する必要がある。

【0124】図19は、新規契約に関する付加情報（ON信号）の送信量と、解約に関する付加情報（OFF信号）の送信量の時間経過に伴う変動を示したものである。新規契約に関する付加情報（ON信号）の送信量と、解約に関する付加情報（OFF信号）の送信量との和が、付加情報の総送信量である。新規契約に関する付加情報の送信は契約数に応じてバースト的な送信量となるのに対して、解約に関する付加情報の送信については、時間の経過とともに解約数を積分したような送信量の変化がみられる。

【0125】新規契約に関する付加情報の送信と、解約に関する付加情報の送信は、いずれもターゲットとする受信装置に確実に受信される保証を欠く。従って、何回か繰り返し放送されるが必要となる。

【0126】放送局側に設置される契約管理装置がON信号、OFF信号となるような付加情報を配信することにより、前述したように、新規契約時と解約時にのみ付加情報を数回繰り返して配信すればよく、契約更新毎に（例えば毎月）全ての加入端末分の契約データを送信する方式と比較して、契約管理情報の送信量を大幅に減少させることが可能である。従って、チャンネルのコンテンツ情報の送信量を増やすことができる。

【0127】（2）受信装置100にて、受信した放送波から、何らかの方法で多重化した付加情報を剥ぎ取ってしまうと、視聴を禁止する付加情報（OFF信号）の

受信を回避して、不正に視聴が行われてしまうこともある。そこで、このような不正行為に対処するため、放送局に設置されている契約管理装置は、一定数のパケット毎に、必ず付加情報を多重化して送信することとする。

【0128】送信すべき付加情報がない場合には、ダミーの付加情報を送信しても良い。この場合、受信装置100のフィルタ503は、パケット数を数えるカウンタ（パケットカウンタ）を具備し、付加情報が到着するとカウンタをリセットする。カウンタの値が、予め定められた数値（N）よりも大となると、異常な状態と判断し、フィルタリング動作を停止するなど、処理中止動作を行う。

【0129】図20に示すフローチャートは、受信装置100のフィルタ503が、上記付加情報の受信状況を監視する処理を伴う場合の処理動作の一例を示したものである。なお、図20において、変数countがパケットカウンタである。

【0130】まず、フィルタ503は、パケットカウンタを初期化する。すなわち、変数countを「0」に設定する（ステップS151）。フィルタ503は、A/D変換部502から順次入力されるパケットに含まれるフラグ情報をチェックする（ステップS152）。

【0131】入力されたパケットのフラグから、当該パケットに付加情報が含まれていると判断した場合は（ステップS153）、パケットカウンタの値を「0」にリセットし（ステップS154）、付加情報用バッファに当該パケットを追加し、順次入力されるパケットのフラグに終了フラグが検出されたら、それまでに付加情報用バッファに格納されたパケットを判定部507に転送する（ステップS155～ステップS157）。

【0132】入力されたパケットのフラグから、当該パケットに付加情報が含まれていないと判断したときは（ステップS153）、パケットカウンタの値を1つインクリメントする（ステップS158）。そして、パケットカウンタの値が予め定められたパケット数Nより大となったときは、異常なパケットの受信状態であると判断し、フィルタリング動作を停止するなど、処理中止動作を行う（ステップS160）。

【0133】一方、ステップS159で、パケットカウンタの値が予め定められた値Nより小さいときは、後続の処理を実行する。

【0134】すなわち、入力されたパケットのフラグから、当該パケットにマスターキーシードが含まれていると判断した場合は（ステップS161）、マスターキーシード用バッファに当該パケットを追加し、順次入力されるパケットのフラグに終了フラグが検出されたら、それまでにマスターキーシード用バッファに格納されたパケットをマスターキー生成部504に転送する（ステップS162～ステップS164）。

【0135】また、入力されたバケットのフラグから、当該バケットにコンテンツ情報、チャンネルサブキーLが含まれていると判断した場合は、当該バケットをチャンネルデコーダ509に転送する（ステップS165）。

【0136】放送局は定期的に（或いは適宜）チャンネルサブキーH又はマスターキーを変更する。チャンネルサブキーHは、チャンネルのコンテンツ情報を暗号化するキー（の構成要素）であるから、チャンネルサブキーHを変更した場合、チャンネルのコンテンツ情報の暗号化も変更を受ける。受信契約を継続する受信装置に対しては、当該

端末IDとチャンネル番号、当該チャンネルのサブキーHを含む付加情報を作成し、放送配信する。

【0137】マスターキーの変更は、契約管理よりも寧ろセキュリティの観点から行われる。マスターキーの変更はマスターキーシードの放送配信による。マスターキーを変更する際は、チャンネルサブキーHも同時に変更することが望ましい。

【0138】（3）図14に示す受信装置100にて受信される放送波には、次のような情報が含まれているものとする。

- ・ マスターキー・シード
- ・ [端末付加情報] Km
- ・ [チャンネル付加情報] Km
- ・ [コンテンツ] Kch

端末付加情報は、各契約ユーザに固有の付加情報で、少なくとも次の情報を含んでいる。

- ・ 端末ID
- ・ チャンネル番号
- ・ 有効／無効情報

なお、契約チャンネルが1つのみの場合、チャンネル番号は含まなくてもよい。

【0139】チャンネル付加情報は、ユーザ少なくとも次の情報を含んでいる：

- ・ チャンネル番号
- ・ チャンネルキー

なお、チャンネル付加情報には、さらにチャンネルキーを識別するためのチャンネルキーIDが含まれていてもよい。

【0140】図14の受信装置の処理動作を図21～図23に示すフローチャートを参照して説明する。

【0141】まず、図21において、受信部501が放送波を受信すると、A/D変換部502がデジタル信号に変換するとともに、当該信号中に含まれる情報をバケット化してフィルタ503に出力する（ステップS101～ステップS102）。

【0142】各バケットは、フラグ情報を有し、このフラグ情報にて当該バケットがマスターキーシードを含むバケットか、端末付加情報あるいはチャンネル付加情報を含むバケットか、コンテンツ情報を含むバケットかを識別することができる。さらに、マスターキーシード、端末付加情報、チャンネル付加情報の最後のバケットには、

終了フラグが記録されている。

【0143】フィルタ503は、マスターキーシード、端末付加情報、チャンネル付加情報それぞれのために、充分な大きさのバッファを有している。

【0144】入力されたバケットのフラグから、当該バケットにマスターキーシードが含まれていると判断した場合は、マスターキーシード用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでにマスターキーシード用バッファに格納されたバケットをマスターキー生成部504に転送する（ステップS103～ステップS106）。

【0145】入力されたバケットのフラグから、当該バケットに端末付加情報が含まれていると判断した場合は、端末付加情報用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでに端末付加情報用バッファに格納されたバケットを判定部507に転送する（ステップS171～ステップS174）。

【0146】入力されたバケットのフラグから、当該バケットにチャンネル付加情報が含まれていると判断した場合は、チャンネル付加情報用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでにチャンネル付加情報用バッファに格納されたバケットを判定部507に転送する（ステップS175～ステップS178）。

【0147】入力されたバケットのフラグから、当該バケットにコンテンツ情報、チャンネルサブキーLが含まれていると判断した場合は、当該バケットをチャンネルデコーダ509に転送する（ステップS111）。

【0148】マスターキー生成部504では、図16のフローチャートと同様である。

【0149】判定部507では、図22のフローチャートに示すように、フィルタ503からバケットが転送されてきたら、まず、マスターキー格納部505からマスターキーKmを読み込み、当該バケットから抽出された付加情報をマスターキーKmを用いて復号する（ステップS181～ステップS183）。

【0150】入力されたバケットのフラグから、当該バケットに端末付加情報が含まれていると判断した場合は、端末付加情報から端末IDを抽出し、ID格納部506に予め格納されている自身の端末IDとを比較し、一致していたときに限り、後続のステップS186以降の処理を実行する。不一致のときは、処理を中止する（ステップS185）。

【0151】ステップS186では、端末付加情報からチャンネル番号とそれに対応する有効／無効情報を抽出し、チャンネル番号に対し「有効」が付随していたときは、ステップS187に進み、当該チャンネル番号のコンテンツ情報の復号／再生が可能なように制御する。その

ために、例えば、各チャンネル毎のオン／オフ制御を行うための配列情報を持ち、有効の場合には、該当するチャンネルの値を「1」とするようにしてもよい。また、チャンネル番号に対し「無効」が付随していたときは、ステップS188に進み、当該チャンネル番号のコンテンツ情報の復号／再生が不可能なように制御する。例えば、上記配列の該当するチャンネルの値を「0」に設定する。

【0152】入力されたバケットのフラグから、当該バケットにチャンネル付加情報が含まれていると判断した場合は、そのチャンネル付加情報からチャンネルキーIDとチャンネルキーを取り出し、当該チャンネル番号に対応させてチャンネルサブキー格納部508に格納する。

【0153】チャンネルデコーダ509では、図23のフローチャートに示すように、フィルタ503から転送されてきたバケットからコンテンツ情報を抽出して、先に取得されたチャンネルキーを用いて復号し、D/A変換部502に出力する（ステップS191～ステップS194）。

【0154】D/A変換部510では、チャンネルデコーダ509から送られてくるコンテンツ情報をアナログ信号に変換し（ステップS195）、再生部511にてアナログ信号の再生を行う（ステップS196）。

【0155】以上説明したように、チャンネル付加情報は全ての受信装置に共通であり、端末付加情報は、チャンネル（サブ）キーを含む場合に比べ短くなるため、付加情報としての契約制御情報を配信するのに必要な放送帯域を節約することが可能となる。

（第2の実施形態）

1）放送システムの概略

契約受信装置に付加情報を放送配信する以外に、図24に示すような配布形態も考えられる。

【0156】図24は、本発明の契約管理装置および放送受信装置を用いた第2の実施形態に係る放送システムの概略構成を示したもので、放送局200から衛星を利用して受信契約を行った各ユーザにコンテンツを提供するサービス形態の場合を示している。

【0157】図24では、契約管理のための付加情報を各契約ユーザに放送配信するのではなく、例えば磁気カード等の携帯可能なカード型の記録媒体（以下、簡単にカードと呼ぶ）Pに記録しておき、それを当該受信装置に宅配又は郵送する点が、前述の第1の実施形態の場合と異なる。契約ユーザは、受信装置100に受け取ったカードPに記録された情報を読み取らせることにより、契約チャンネルの受信が可能となる。

【0158】2）契約管理装置

図25は、第2の実施形態に係る契約管理装置の構成例を示したもので、図3と同一部分は同一符号を付し、異なる部分について説明する。すなわち、図3の放送装置13が図25では、カード作成装置15に置き換えられ、付加情報を地上波あるいは衛星放送を介して配信す

るのではなく、磁気カード、ICカード等のカード型記録媒体（カード）に記録して、契約ユーザに配布するようになっている。

【0159】付加情報生成制御部9からの指示が「1997年12月1日から4ヶ月間契約している契約ユーザの付加情報を送れ」であった場合、前述の図3に示した構成の契約管理装置では、付加情報を1ヶ月毎に作成しなくてはならないために1ヶ月毎に有効なチャンネルキーと有効なマスターキーを検索して、図8のフローチャートに示す処理を行う必要がある。図25に示す契約契約管理では、付加情報を放送によらずに例えば磁気カードに4ヶ月分の契約チャンネルのチャンネルキーに対応する付加情報を書込み、当該ユーザに配送すればよい。これにより、1ヶ月毎の配信、配布を行わなくてもよく、放送局側にもユーザ側にも煩雑を避ける意味で有利である。

【0160】2）受信装置

図26は、第2の実施形態に係る受信装置100の構成例を示したもので、前述の図25に示したような放送局側に設置されている契約管理装置で作成されたカードから付加情報の読み取り、図10に示したようなコンテンツ情報の配信装置から出力される放送波を受信するためのものである。なお、図14と同一部分には同一符号を付している。

【0161】ここで、図26に示す受信装置100にて受信される放送波には、次のような情報が含まれているものとする。

- ・ マスターキーシード
- ・ チャンネルサブキーL
- ・ チャンネルサブキーID
- ・ 「コンテンツ」Kch

チャンネルサブキーIDは、付加情報の中のチャンネルサブキーを識別するためのIDで、チャンネルサブキーの変更が必ずマスターキーの変更を伴う場合には不要である。

【0162】カードPには、マスターキーにて暗号化された付加情報が記録されている。

【0163】付加情報は、次のような情報が含まれているものとする。

- ・ 端末ID
- ・ チャンネル番号（複数可）
- ・ チャンネルサブキーID
- ・ チャンネルサブキーH

なお、付加情報には、さらに、判定部507にてマスターキーによる復号が正しく行われたか否かを判定するための認証コード（例えば、予め定められた適当なビット列でもよい）が含まれていてもよい。

【0164】カードPに記録されている付加情報は1つとは限らない。契約期間がマスターキーやチャンネルサブキーHの更新時期にまたがる場合、チャンネルサブキーHと暗号化のキーの異なる付加情報が複数記録されていてもよい。

【0165】図27は、カードPに記録される付加情報の例を示したもので、図27(a)では、マスターキーKmとチャンネルサブキーHの更新時期が同じ場合(例えば、1ヶ月毎)、図27(b)は、マスターキーKmの更新時期が例えば2ヶ月毎であるのに対し、チャンネルサブキーHの更新時期が1ヶ月毎である場合に、それぞれユーザが2チャンネル(チャンネル番号X、Y)を3ヶ月視聴する契約を行ったときにカードPに記録される付加情報を示している。

【0166】図27(a)に示すように、マスターキーKmとチャンネルサブキーHの更新時期が同じ場合、各月毎のチャンネル毎のチャンネルサブキーHを各月毎のマスターキーKmで暗号化した3つの付加情報が記録されている。この場合、各チャンネル毎のチャンネルサブキーは1つのみなので、チャンネルサブキーIDは必ずしも必要ない。

【0167】図27(b)に示すように、マスターキーKmとチャンネルサブキーHの更新時期が異なる場合、1つのマスターキーで暗号化されて生成される付加情報には、契約期間に応じて、各チャンネル毎に複数(例えば2ヶ月分)のチャンネルサブキーが記録されている場合もある。その場合、各チャンネルサブキーはチャンネルサブキーIDにてそれぞれ識別されている。

【0168】なお、図27(a)、(b)のいずれにおいても1つのマスターキーで暗号化される情報単位には認証コードが含まれていてもよい。

【0169】次に、図26の受信装置の処理動作を図28～図30に示すフローチャートを参照して説明する。ここでは、カードPに記録されている付加情報が例えば図27(b)に示すような場合を例にとり説明する。

【0170】まず、図28に示すように、放送局側から配送されたカードPをユーザがカードリーダー513に挿入する。カードリーダー513は、挿入されたカードPから付加情報を読み取り、付加情報格納部512に格納する(ステップS201)。

【0171】図29の説明に移り、受信部501が放送波を受信すると、A/D変換部502がデジタル信号に変換するとともに、当該信号中に含まれる情報をバケット化してフィルタ503に出力する(ステップS101～ステップS102)。

【0172】各バケットは、フラグ情報を有し、このフラグ情報にて当該バケットがマスターキーシードを含むバケットか、チャンネルサブキーIDを含むバケットか、コンテンツ情報を含むバケットかを識別することができる。さらに、マスターキーシードの最後のバケットには、終了フラグが記録されている。

【0173】フィルタ503は、マスターキーシード、付加情報のそれぞれのために、充分な大きさのバッファを有している。

【0174】入力されたバケットのフラグから、当該バ

ケットにマスターキーシードが含まれていると判断した場合は、当該バケットを判定部507へ出力する(ステップS211～ステップS213)。

【0175】入力されたバケットのフラグから、上記以外のバケット、すなわち、当該バケットにコンテンツ情報、チャンネルサブキーLが含まれていると判断した場合は、当該バケットをチャンネルデコーダ509に転送する(ステップS213)。

【0176】マスターキー生成部504の処理は、図16のフローチャートと同様である。

【0177】次に、判定部507では、図30のフローチャートに示すような処理を実行する。カードPに記録されている付加情報は1つとは限らない。そこで、変数iをカードPに記録されている複数の付加情報のインデックスに用い、付加情報中に含まれる、マスターキーによる復号が正しく行われた否かを判定するための認証コードのチェックをもって、有効な付加情報とみなすことにする。

【0178】まず、変数iの値を「0」にセットしてから(ステップS221)、付加情報格納部512に格納されている付加情報を1つずつ読み出す(ステップS222)。そして、マスターキー格納部505に格納されているマスターキーを読み出して(ステップS224)、付加情報を復号する(ステップS225)。復号された付加情報中に認証コードが含まれている場合は、その認証コードが正しいものであるか否かを確認する(ステップS226)。

【0179】認証コードが正しいものであるときは、契約期間内の正当なマスターキーで復号された有効な付加情報であると判断できる。従って、その付加情報に基づきステップS228以降の判定処理を実行する。一方、認証コードが誤ったものであるときは、変数iを1つインクリメントして(ステップS227)、付加情報格納部512に格納されている次の付加情報を読み出し、上記ステップS222～ステップS226を繰り返す。

【0180】ステップS228では、付加情報から端末IDを抽出し、ID格納部506に予め格納されている自身の端末IDとを比較し、一致していたときに限り、後続の処理を実行する。不一致のときは、処理を中止する。

【0181】次に、フィルタ503から転送されてきたバケットからチャンネル番号毎のチャンネルサブキーIDを抽出し、さらに、付加情報からチャンネル番号毎のチャンネルサブキーIDを1つずつ取り出し、それを比較する(ステップS229)。一致していたら、付加情報から当該チャンネルサブキーIDに対応するチャンネルサブキーHを抽出し、チャンネルサブキー格納部508へ格納する(ステップS231)。不一致のときは、付加情報から当該チャンネル番号の次のチャンネルサブキーIDを取り出して(ステップS230)、再び、先にバケットから抽

出されたチャンネルサブキーIDと比較すればよい。

【0182】チャンネルデコーダ509、D/A変換部510、再生部511の処理動作は、図18のフローチャートと同様である。

【0183】(用語の説明)以下の実施形態について述べる前に用語の定義を行なう。限定受信を行なうためチャンネル毎の契約状態を記述した情報を契約情報と呼ぶ。例えば各チャンネルにチャンネル番号を付け、チャンネル番号に対応したビットが「1」であるか否かによりチャンネルの契約状態を表すことができる。これを特にチャンネル契約情報という。

【0184】契約情報には、これ以外にも様々な形態があり得る。例えば、図11(b)のチャンネルサブキーHとチャンネル番号の組も当該チャンネル番号のチャンネルが契約されていることを示す契約情報であり、図12のチャンネル番号と有効/無効の情報の組も当該チャンネル番号の契約状態を示す契約情報である。

【0185】契約情報は受信装置IDと相互にリンクされており、受信装置IDは、当該契約情報が適応される受信装置の識別子を示している。この意味で契約情報と受信装置IDは一体のものであり、受信装置IDと契約情報の組を単に契約情報と呼ぶこともある。今後両者を区別する必要がある時には、前者を狭義の契約情報、後者を広義の契約情報として区別する。

【0186】また、以下の実施形態では、契約情報(契約情報と受信装置IDの組)は(改竄を防いだり、不利な契約情報の取得を防ぐ目的で)暗号化されて放送配信もしくは磁気カード等の記録媒体に記載され郵送等で送られるが、ここで契約情報と一緒に暗号化されるデータセットをまとめて受信契約情報と呼ぶことにする。受信契約情報には、契約情報も含まれる。更に受信契約情報にデータの識別子など本システムに必要な情報を付加したものを契約情報パケットという。

【0187】実施形態は、チャンネルキーと契約情報の分離の程度によって分類されている。即ち、受信契約情報にチャンネルキーをどの程度含めるかによって区別される。

【0188】前述の第1の実施形態は、受信契約情報の中にチャンネルキーの一部が含まれることを特徴とする請求項4に記載の放送受信装置に対応する実施の形態である。

【0189】前述の第2の実施形態は、受信契約情報の中にチャンネルキーを1ビットも含まないことを特徴とする請求項2に記載の放送受信装置に対応する実施の形態である。

【0190】第3の実施形態は、受信契約情報の中に暗号化されたチャンネルキーを復号するためのチャンネルキー復号鍵が含まれることを特徴とする請求項3に記載の放送受信装置に対応する実施の形態である。

【0191】第4の実施形態は、受信契約情報の中にチ

ャネルキーそのものを含めることを特徴とする請求項5に記載の放送受信装置に対応する実施の形態である。

【0192】第5の実施形態は、課金制御部(課金チップ)の製造上必要なテスト用スキャンバスラッチ部の構成を示したもので、第1~4の実施形態に共通に利用できる技術である。

【0193】なお、第3の実施形態以降の説明において、放送受信装置内部で限定受信の仕組みを実現する構成部を課金制御部と呼ぶ。なお、課金制御部はハードウェアにて構成され、しかもLSI化されているものが望ましい。このようなLSI化された課金制御部を課金チップと呼ぶのもよい。いずれにしても、課金制御部には限定受信のための秘密情報が含まれているので内部のメモリやハード構成に関して外部から容易に読み出し、書き込み、変更ができない耐タンパ構造を仮定している。

【0194】また、課金制御部内部のメモリには全ての放送受信装置に共通のマスター鍵が書き込まれており、主に受信契約情報を復号するのに用いられる。また、受信装置IDは、放送受信装置毎個別に設定され、課金制御部内部の不揮発性メモリの中に記録されている。

【0195】第1の実施形態と第2の実施形態においては上記の用語が次のような形で述べられている。すなわち、受信契約情報を付加情報、課金制御部を復号ユニット、受信装置IDを端末ID。

【0196】また、第1の実施形態と第2の実施形態で述べられているチャンネル番号、フラグ情報は、それぞれ、第3の実施形態と第4の実施形態で述べられているチャンネル識別子、情報識別子にあたる。

【0197】(第3の実施形態)

1) 放送受信装置

図31は、本実施形態に係る放送受信装置の構成を概略的に示したものである。

【0198】本実施形態の放送コンテンツは図32に示すように4段の暗号化機構によって保護されている。チャンネルキーKchは、スクランブルされた放送コンテンツを復号するための鍵であり、一般にチャンネル毎に異なり、短期間で変更される。

【0199】図33に示すように放送波には2種類の情報(放送コンテンツ情報、チャンネルキー情報)が含まれている。ここで放送コンテンツのデスクランブルはチャンネルキー情報から得られたチャンネルキーKchで行なわれる。

【0200】さて、図32の説明に戻り、チャンネルキー情報に含まれるチャンネルキーKchは暗号化されており、チャンネルキー復号鍵KHで復号できる。このチャンネルキー復号鍵KHはチャンネルに依存しない、システム共通のもので、暗号化された受信契約情報に含まれている。

【0201】暗号化された受信契約情報は、予め全ての放送受信装置に共通に存在するマスター鍵KMで復号さ

れる。更にマスター鍵 K_M は、マスター鍵シード S_M によって定期的に更新される。

【0202】スクランブル放送波をデスクランブルするためには、チャンネルキー K_{ch} を取得しなくてはならず、取得のためには暗号化されたチャンネルキーを復号する必要がある、その復号鍵 K_H は、暗号化された受信契約情報に含まれている。暗号化された受信契約情報は、マスター鍵 K_M で復号される。また、マスター鍵で復号された受信契約情報の中には、受信装置IDに対応付けられた各受信装置宛の狭義の契約情報も一緒に含まれており、放送受信装置はこれを自分のものであると判断した上で取得し、契約情報格納部にこれを格納する。

【0203】放送受信時には、契約情報格納部から契約情報を参照し、当該チャンネルが契約済であった場合のみ前記の手段で取得したチャンネルキー K_{ch} をデスクランブル部に送り、放送波をデスクランブルする。

【0204】このようなシステムを取ることににより、チャンネルキー K_{ch} を取得するためにチャンネルキー復号鍵 K_H を取得しなければならず、更に契約情報とチャンネルキー復号鍵 K_H が受信契約情報の暗号化により不可分になるので、チャンネルキー復号鍵 K_H を取得するためには、契約情報を取得しなければならなくなり、契約を確実に遵守させることが可能となる。

【0205】以下では更に詳しく説明する。本実施形態の放送受信装置で受信されるチャンネルには、通常チャンネルと契約情報チャンネルがあり、通常チャンネルには通常の放送コンテンツが流れている。その構造は、図33に示す通りである。ここで、放送コンテンツ情報は、図34に示すように、暗号化された放送コンテンツ(C)とチャンネルキー識別子(KID)とチャンネル識別子(CID)と情報識別子(IID)とに分かれる。

【0206】ここで、情報識別子とは当該情報が放送コンテンツ情報であることを示すもので、例えば、「0001」であってもよい。また、チャンネル識別子は、当該放送コンテンツがどのチャンネルのコンテンツであるかを識別するための情報である。更に、チャンネルキー識別子は、当該暗号化コンテンツを復号することができるチャンネルキーを識別するための情報である。この利用法及び構造は後で詳しく述べる。

【0207】一方、チャンネルキー情報は、図35に示すように、暗号化されたチャンネルキーとチャンネルキー識別子、チャンネル識別子、チャンネルキー復号鍵識別子及び情報識別子からなっている。

【0208】ここでチャンネルキー識別子は当該チャンネルキーを識別するための情報で暗号化コンテンツを復号する際に利用される。チャンネル識別子は当該チャンネルキーで復号できるコンテンツ情報のチャンネルを示す情報である。チャンネルキー復号鍵識別子は暗号化されたチャンネルキーの復号鍵を識別するために用いられる。この利用法及び構造は後で詳しく述べる。情報識別子は当該情報が

チャンネルキー情報であることを示すもので、放送コンテンツ情報等の他の情報と区別するために、例えば「0002」であってもよい。

【0209】契約情報チャンネルの構造は図36に示す通りで、契約情報バケットとマスター鍵シードからなる。

【0210】ここで、契約情報バケットは図37に示すように、暗号化された受信契約情報、チャンネルキー復号鍵識別子、マスター鍵識別子、情報識別子からなっている。

10 【0211】チャンネルキー復号鍵識別子は、当該受信契約情報に含まれるチャンネルキー復号鍵を識別する情報で、暗号化されたチャンネルキーを復号する際の復号鍵の識別に用いられる。マスター鍵識別子は当該契約情報バケットに含まれる暗号化受信契約情報が復号できるマスター鍵を識別するために用いられる。情報識別子は当該情報が契約情報バケットであることを示すもので、例えば「0003」であってもよい。

20 【0212】受信契約情報は、図38に示すように、受信装置ID、チャンネル契約情報、チャンネルキー復号鍵 K_H からなっている。受信装置IDは当該受信装置に固有の識別子(ID)であり、当該契約情報が当該受信装置宛のものであるか否かの判定に用いる。チャンネル契約情報はユーザに提供可能な複数のチャンネルのそれぞれに1ビットずつ割り当て、当該ユーザが契約しているチャンネルに該当するビットは「1」、そうでないビットには「0」を割り当てることにより、当該受信装置の契約状態を表す。チャンネルキー復号鍵 K_H は、チャンネルキー K_{ch} を復号するための鍵である。

30 【0213】マスター鍵シード情報は、図39に示すように、マスター鍵シードとマスター鍵識別子、情報識別子からなっている。マスター鍵シードはマスター鍵を生成するためのシード情報である。マスター鍵識別子は当該マスター鍵シードで生成されたマスター鍵の識別情報である。情報識別子は当該情報がマスター鍵シード情報であることを示すためのものであり、例えば「0004」としても良い。

【0214】ここでチャンネルキー識別子の役割について述べる。

40 【0215】放送コンテンツ情報は、図34に示すように、チャンネルキーによって暗号化された放送コンテンツ情報Cとチャンネルキー識別子KIDとチャンネル識別子CIDと情報識別子IIDよりなる。チャンネルキー識別子KIDは、暗号化された放送コンテンツ情報Cがどのチャンネルキーで暗号化したものかを示すもので、チャンネルキーに固有に付けられた識別子(ID)である。この場合、スクランブル放送コンテンツを復号するチャンネルキーは一意に決まるので系統的に明解である。

50 【0216】しかし、実装上は当該チャンネルキーを何時の時点まで保持しなくてはならないかが明確でないばかりか、IDを一意的にするためIDの長さが長くなり、

大きな記憶容量を要するなどの問題がある。そこで、ここでは1ビットの相対IDを付ける例を考える。即ち、(暗号化して)送信するチャンネルキーに対して(交互に)「0」もしくは「1」という1ビットのIDを付け、新しいチャンネルキーを受信したら、(図41に示すような)メモリ上のチャンネルキーを更新して行く。

【0217】この際、(当然のことながら)新しいチャンネルキーはそれに対応するスクランブル放送波の送信に先立って送られなくてはならない。このため送信のスケジュールは、全ての放送受信装置で鍵の復号とメモリへの格納が完了する時間を考え、図40のようにチャンネルキー切替え時点でチャンネルキー「0」とチャンネルキー「1」の送信がオーバーラップする時間帯(Tx1、Tx2)が存在する。この時間帯をどれだけ取るかは放送受信装置が暗号化チャンネルキーを復号して、メモリに格納する時間をどれだけに見積もるかによっている。このようにすることにより、チャンネルキーのIDに相対IDを用いることができる。

【0218】鍵の相対IDの概念は本実施形態における他の全ての鍵(チャンネルキー復号鍵、マスター鍵)にも同様の方式で用いることができる。

【0219】次に、図31に示した放送受信装置の構成と、その処理動作について、図42～図45に示すフローチャートを参照して説明する。

【0220】放送波は、チャンネルに関わらず受信部1101で受信される(図42のステップS1001)。受信された放送波はA/D変換部1102でA/D変換され(ステップS1002)、誤り検出/訂正部1103で誤り訂正符号などを用いることにより、伝送途中で載ったノイズ等の除去を行なう(ステップS1003、ステップS1004)。

【0221】ノイズが除去された放送波は、チャンネル選択部1104に送られ、例えば、通常のテレビ受信機と同様なチャンネルを選択するためのチャンネル選択インターフェース(I/F)1105などを用いて選択されたチャンネルに対応した放送波と契約情報チャンネルの放送波を課金制御部1106に送る。

【0222】課金制御部1106では、これをフィルタ一部1107に送り、放送コンテンツ情報とチャンネルキー情報と契約情報バケット及びマスター鍵シード情報に分離する。この分離は各々の情報識別子によって行なう。

【0223】さて、受信した情報がマスター鍵シード情報であれば(ステップS1013)、これはフィルタ一部1107から分離され、マスター鍵生成部1111に入力される(ステップS1014)。マスター鍵生成部1111ではマスター鍵シード情報からマスター鍵シードとマスター鍵識別子を分離し、マスター鍵シードから乱数生成や暗号化のアルゴリズムを用いてマスター鍵を生成し(ステップS1015)、マスター鍵識別子(例

えば、相対IDで「0」または「1」)に示されたメモリに格納する(ステップS1016)。

【0224】ここで生成アルゴリズム及び乱数生成のための秘密情報は全ての放送受信装置及び放送局に共通であり、課金制御部1106内の不揮発性メモリか外部からアクセスできないROMに秘匿されている。このため暗号化されていないシードを送っても1つのマスター鍵を共有することができるのである。

【0225】受信した情報が契約情報バケットであれば(ステップS1011)、フィルタ一部1107から契約情報復号部1110へ送られる(ステップS1012)。契約情報復号部1110では、契約情報バケットに含まれているマスター鍵識別子に対応するマスター鍵をマスター鍵格納部1112から取得する(ステップS1041)。この時マスター鍵格納部1112に対応するマスター鍵が存在しない場合は、その時点で処理を終了する。ここで「NULL」(全てのビットが「0」)のマスター鍵は存在しないと仮定し、「NULL」が取得された場合にマスター鍵が格納されていないと判断しても良い。

【0226】マスター鍵が出力された場合(ステップS1042)、契約情報バケット内にある暗号化された受信契約情報を当該マスター鍵で復号する(ステップS1043)。復号された受信契約情報の中から受信装置IDを取得し、認証部1114は、それを受信装置ID格納部1113に格納されている受信装置IDと比較する(ステップS1044)。もし、一致したら(ステップS1045)、当該受信装置IDとリンクされたチャンネル契約情報をチャンネル契約情報格納部1116に格納する(ステップS1046)。一致した場合でもしない場合でも、チャンネルキー復号鍵K_Hは当該契約情報バケットに含まれるチャンネルキー復号鍵識別子(例えば、相対IDで「0」または「1」)に示されたメモリに格納する(ステップS1047)。

【0227】受信した情報がチャンネルキー情報であり(図42のステップS1008)、さらに、当該チャンネルキー情報中のチャンネル識別子をチェックして、チャンネル選択I/F1105で選択されたチャンネルのチャンネルキー情報であるときは(ステップS1009)、フィルタ一部1107からチャンネルキー復号部1109へ送られる(ステップS1010)。

【0228】チャンネルキー復号部1109では、チャンネルキー情報に含まれるチャンネルキー復号鍵識別子に対応するチャンネルキー復号鍵をチャンネルキー復号鍵格納部1115から取得する(図44のステップS1031)。ここでもマスター鍵取得の時と同様に、「NULL」のチャンネルキー復号鍵が取得された時は、まだチャンネルキー復号鍵が格納されていないと判断し、そこで処理を終える。「NULL」でないチャンネルキー復号鍵が取得された場合は(ステップS1032)、それを使ってチャ

ネルキー情報に含まれる暗号化チャンネルキーを復号する（ステップS1033）。

【0229】復号されたチャンネルキーはチャンネルキー情報に含まれるチャンネルキー識別子（例えば、相対IDで「0」または「1」）に示されたメモリへ格納する（ステップS1034）。

【0230】受信した情報がスクランブル放送コンテンツ情報であり（図42のステップS1005）、さらに、当該放送コンテンツ情報中のチャンネル識別子をチェックして、チャンネル選択I/F1105で選択されたチャンネルの放送コンテンツ情報であるときは（ステップS1006）、フィルター部1107からデスクランブル部1108へ送られる（ステップS1007）。

【0231】デスクランブル部1108では、チャンネルキー出力部1120へチャンネル識別子を送り、当該チャンネルのチャンネルキーを取得する（ステップS1021）。チャンネルキー出力部1120は、契約判定部1118に当該チャンネルが契約済みかどうかを問い合わせる。これを受けて契約判定部1118は、チャンネル契約情報格納部1116のチャンネル契約情報を参照して、当該チャンネルが契約済みか判定し、契約済の場合「1」、未契約の場合「0」を出力する。チャンネル契約情報は例えば、契約済みの場合「1」、未契約の場合「0」といったものでよい。

【0232】契約判定部1118から「0」が出力された場合は、チャンネルキー出力部1120は「NULL」をデスクランブル部1108に出力して、契約されていないことを示す。契約判定部1118から「1」が出力された場合、チャンネルキー出力部1120は、チャンネルキー格納部1117からチャンネルキー識別子に対応するチャンネルキーを取得する。ここでもマスター鍵取得の時と同様に「NULL」のチャンネルキーが取得された時は、まだチャンネルキーが格納されていないと判断し、そこで処理を終える。「NULL」でないチャンネルキー復号鍵が取得された場合は（ステップS1022）、デスクランブル部1108は、それを使ってスクランブル放送コンテンツを復号し、出力する（ステップS1023、ステップS1024）。

【0233】なお、受信装置ID格納部1113は、課金制御部1106内の耐タンパな不揮発性メモリで構成され、受信装置IDが課金制御部1106外へ出力されることがないことが望ましい。そのような課金制御部1106であれば受信装置IDを読み取ることは極めて困難なので契約情報を偽造することは事実上不可能とすることができる。また、マスター鍵についても同様の耐タンパ性を仮定すれば、課金制御部1106内のメモリから読み取って、送信されてくる契約情報パケットに含まれる受信契約情報を端から復号し、当該放送受信装置に不利な（当該受信装置の）受信契約情報を含む契約情報パケットのみをカットする攻撃も不可能となる。

【0234】また、課金制御部1106に対して十分な耐タンパ性を仮定すれば、マスター鍵は読み出されることはないので、マスター鍵シードを送ってマスター鍵を変更する必要もなくなる。この場合、マスター鍵は固定になるので本実施形態に関してマスター鍵シードを入力して、マスター鍵を変更する部分の構成を削ることができる。

【0235】さらに、マスター鍵を格納するマスター鍵格納部1112は、受信装置ID格納部1113と同様に、課金制御部1106内の耐タンパな不揮発性メモリで構成されていてもよいし、課金制御部1106内の回路として設定されていても良い。このようにすることにより、回路規模が削減できる。

【0236】しかし、ハードウェアの耐タンパ性は現在のところ完全なものは存在しない、即ち、耐タンパ性にはレベルがあり、ハードウェア内部のメモリや回路の内容の読み込み書き込みが、容易に手に入りしかも安価な装置を使って実現できるレベルのものから、本格的な装置を使って一定の技術を持った者が時間を掛けなければできないものまで様々である。従ってコストとの兼ね合いの観点から課金制御部1106に強い耐タンパ性を持つハードウェアを利用できない場合もある。このためあまり強い耐タンパ性を仮定せず、システム側で耐タンパ性を補強することは重要である。

【0237】耐タンパ性が崩壊した場合、課金制御部1106内に秘匿されているマスター鍵と受信装置IDが読み取られる可能性がある。その場合、契約情報の偽造が可能である。これを防ぐため次のような工夫は重要である。

【0238】契約情報の偽造を防ぐには、公開鍵方式が有用である。公開鍵方式は例えば放送局側で秘密鍵を使って暗号化データを作り、課金制御部1106内にある公開鍵によってそのデータを処理することができる方式である。ここで、公開鍵から秘密鍵を算出することが計算量的に極めて困難で、事実上不可能なことから、秘密鍵を知らない者が公開鍵で復号して意味のあるデータを作成することができないところに特徴がある。即ち、契約者が自分に都合の良い暗号化された受信契約情報を作成しようと思っても、秘密鍵を知らないので極めて困難となるのである。この意味で受信契約情報の暗号化に公開鍵暗号を用いることは有用である。

【0239】さらに、受信契約情報に公開鍵暗号によるデジタル署名を含めるという構成も有用である。デジタル署名とは、受信契約情報からデジタル署名を除いた部分にハッシュ関数というある種の要約関数を施して要約した値（これをハッシュ値という）に対して秘密鍵を使って暗号化したものである。デジタル署名は前記同様秘密鍵を知らない事実上作成できないばかりか、公開鍵によってデジタル署名を復号し得られたハッシュ値と、別途受信契約情報からデジタル署名を除いた部分に対す

るハッシュ値を比較することによりデジタル署名を検証することが可能である。

【0240】この場合、デジタル署名の検証は当該受信装置IDが受信契約情報の中に存在した時のみに行なうことにすると良い。何故ならデジタル署名の検証には時間がかかり、基本的に契約情報を更新する必要がある場合以外、署名の検証を行う必要はない。

【0241】受信契約情報にデジタル署名を付けたときの放送受信装置の構成は、図31における認証部1114を図68に置き換えれば良い。その場合の受信契約情報の構成を図69に示す。勿論、後述する図49に示すように、データ圧縮も可能である。しかし、前記の手段を取っても次のような攻撃法は可能である。即ち、一旦全てのチャンネルに対して契約した契約者が、その時送信された契約情報パケットを記録しておく。ここで、契約者がマスター鍵と受信装置IDを知っていれば当該放送受信装置の契約情報を特定することができるが、例えばそれらを知らなくても契約情報放送波を記録しておき、視聴が可能になる前の一定期間に当該放送受信装置に対する契約情報を含む契約情報パケットが流れたと考えるの自然である。次に契約者は全チャンネルを解約し、そのため全チャンネルは視聴できなくなるが、視聴できなくなった時点で先に記録した古い暗号化受信契約情報を含む契約情報パケットを再び何らかの手段で課金制御部1106に入力して以前の(有利な)契約情報に置き替えてしまうことは原理的には可能である。しかも、この場合はデジタル署名も正しいので放送受信装置は契約情報を受信してしまう。このような攻撃を防ぐためには定期的にデジタル署名用の公開鍵を変更する必要がある。変更してしまえば古いデジタル署名は無効になる。変更の仕方は情報識別子を使うことにより情報を識別し、パケット内のデジタル署名用公開鍵を不揮発性メモリに格納すれば良い。この鍵は公開鍵であるため特に暗号化する必要はないが、機密保持のためマスター鍵で暗号化する構成も考えられる。

【0242】また、次々と送られてきて即時に復号化されなければならない放送コンテンツに関して、暗号化は共通鍵暗号が望ましい。これは共通鍵暗号が公開鍵暗号よりも、100倍～1000倍高速であるからである。チャンネルキーの暗号化にも同様に共通鍵暗号が望ましい。

【0243】更に、マスター鍵生成部1111の入力となるマスター鍵シードであるが、これは文字通り乱数のシードでも良いが、共通鍵暗号や公開鍵暗号を使って暗号化したマスター鍵であっても良い。その場合それらのための復号鍵が課金制御部1106内に耐タンパな不揮発性メモリもしくは回路として記録されていないといけない。

【0244】本実施形態のチャンネルキー格納部111

7、チャンネルキー復号鍵格納部1115、マスター鍵格納部1112は、放送受信装置の電源オフ時に「NULL」にクリアされなくてはならない。何故なら再び電源をオンする時には、これらの鍵は変更されている可能性が高いからである。NULLクリアされていれば、当該キーがまだ格納されていない場合は復号動作が起きないので、対応しない鍵で復号してしまって無意味なデータを出力する心配はない。

【0245】また、上記事項に関連して間違ったチャンネルキー情報を課金制御部1106が受けとってしまった場合を考えよう。勿論誤り訂正符号を用いた誤り検出/訂正は、誤り検出/訂正部1103で行われるのであるが、それでも確実ではない。もし、誤った鍵情報(例えば、チャンネルキーもしくはマスター鍵シード)のまま課金制御部1106が受け取ってしまえば、誤った鍵や契約情報を格納し、それを使って誤った復号や限定受信が行なわれる。一般に暗号は鍵が1ビットでも違えば復号結果は正しい結果とはかけ離れてしまう。これは、鍵から平文(元のデータ)が類推できないという安全性の要求からきたものであり、このような性質を持っていない暗号は弱い暗号なので利用できない。そこで暗号化した鍵情報や契約情報を含む重要な情報に認証子をつける方式が考えられる。

【0246】次に、図46～図48を参照して、暗号化された鍵情報や契約情報を含む重要な情報に認証子を用いた場合について説明する。暗号化した鍵情報に付ける認証子は、復号した結果得られる鍵情報から何らかのアルゴリズムで演算されるものである。そのため復号した結果から認証子を求める演算を施して得られたものと認証子を比較して一致していれば誤りのないデータと考える訳である。ここで認証子は、例えば鍵kを鍵kで暗号化したものの上位32ビットなどとしても良い。ここで鍵を64ビットと仮定すれば、認証子は最大64ビットとなる。当然だがこの方式では誤り検出しかできない。

【0247】また、誤りがあっても検出に失敗してしまう確率は認証子の長さによって決まり、認証子の長さを1とすると、 $1/2^l$ である。これは認証子が長ければ長いほど失敗確率が減ることを意味している。即ち要求される失敗確率によって認証子の長さを決めれば良いことになる。その意味で要求される失敗確率が相対的に低く、64ビットの認証子では間に合わない場合もあるだろう。この場合は別系統の認証子を更に付ける必要がある。別系統の認証子とは基本的に別のアルゴリズムで作った認証子であるが、その実現が困難な場合は、現在のアルゴリズムを使って、鍵kをある一定の関数で変換した後、同じアルゴリズムで作成したものを認証子とする。もしくは最初に得られた認証子に対して更に同じアルゴリズムを掛けて認証子を生成することができる。認証子生成アルゴリズムに暗号アルゴリズムを使うと表面的なビット列として相互に関係がない認証子を作ること

ができる。これは、暗号アルゴリズム自体にランダム性があるからである。殆ど「0」に近い失敗確率を求められた場合はこのようにして十分多くの認証子を用意し、それを一定の手段で縮めたものを用いれば良い。

【0248】本実施形態において認証子付きの暗号化鍵情報を考える場合は、暗号化鍵情報の部分を図46に置き換え、図31におけるチャンネルキー復号部1109、契約情報復号部1110（もしくは認証部1114）の内部にそれぞれ認証子確認部を設け、認証に失敗した場合は、鍵を出力しないように構成すれば良い。

【0249】受信契約情報やマスター鍵シードにも認証子を付ける必要があるが、ここでマスター鍵には公開鍵暗号系も考えられるので64ビットのように区切れの良いブロックになっていない。公開鍵暗号系の鍵は共通鍵暗号系の鍵よりも長いので図47に示すようにブロックに区切り、それぞれのブロックで上記の手段で認証子を作り、それらの認証子同士の排他的論理和（EXOR）をとるなどという手段で認証子を作ることが可能である。

【0250】また、受信契約情報に鍵情報（本実施形態の場合はチャンネルキー復号鍵）が含まれる場合は、その鍵情報を使って上記ブロック分割でできた各ブロックを暗号化し、上記同様にして排他的論理和（EXOR）を取って認証子を作ることができる。

【0251】また、図48に示すように、第1ブロックの第1の認証子を前記の例と同じ手法で作り出して、第2ブロックと排他的論理和（EXOR）を取る。排他的論理和を取ったものに対して前記のアルゴリズムで第2の認証子を作る。これを繰り返すことによって最終的に認証子が生成される。いずれの場合も、64ビットにブ
30 ロック化するために、必要に応じて図47に示したようなPADというNULLデータ（疑似データ）を入れる。従って、マスター鍵シードに認証子を付ける場合もマスター鍵生成部1111の中に認証子を確認するプロセスを入れればその検証を実現できる。

【0252】最後に、受信契約情報の構成の拡張について触れておく。受信契約情報は、図38に示すように、受信装置ID（TID）とチャンネル契約情報（CHS）とチャンネルキー復号鍵から構成されている。

【0253】チャンネルキー復号鍵は安全性確保のためにチャンネルキーよりも鍵サイズを長くとしている。例えばDES（Data Encryption Standard）などの標準的な暗号を用いるとチャンネルキーは64ビット、チャンネルキー復号鍵は128ビットのように構成される。ここで、受信装置ID（TID）は放送受信装置をユニークに定めれば良いので高々50ビット程度でよい。チャンネル契約情報（CHS）は、チャンネル数だけのビットが必要だが例えば30チャンネルあれば30ビットで良い。従ってチャンネルキー復号鍵以外の部分
40 は80ビットで半分以上はチャンネルキー復号鍵が占め

る。

【0254】ところでチャンネルキー復号鍵は全ての放送受信装置に共通であり、受信契約情報（少なくとも、受信装置IDとチャンネル契約情報を含む）の受信を確実にするために受信契約情報に入れてある。何故なら、自分に不利な受信契約情報でもチャンネルキー復号鍵が含まれていれば受信せざるを得ないからである。この主旨からは1つの契約情報パケットに複数の放送受信装置に対する受信契約情報を入れても問題はなく、その方が送信データが少なくなるのである。

【0255】そこで、図49に示すように、契約情報パケットを構成する。なお、図49では、契約情報パケット中の受信契約情報に関する部分のみを示している。

【0256】ここではチャンネルキー復号鍵の両側に対応する受信装置ID（TID）とチャンネル契約情報（CHS）の組を複数配置している。ここで契約情報パケットの先頭部分にチャンネルキー復号鍵を配置しないのは、受信契約情報の暗号化にDESのような共通鍵暗号を使った場合、64ビットを1ブロックとしてその単位で暗号化することが多いため、チャンネルキー復号鍵が128ビットであった場合、最初の2ブロックがチャンネルキー復号鍵である。もし、このことが分かると、受信機を改造して最初の2ブロックのみを復号し、チャンネル契約情報を取得せずにチャンネルキー復号鍵を取得することが可能になる。同様のことは、チャンネルキー復号鍵を最後に配置した場合にも言える。ただし、64ビット単位ではない公開鍵暗号のような暗号系で暗号化する場合はこの限りではない。また、いずれの場合も暗号化ブロックの切れ目がデータの切れ目と一致しないようにすることが望ましい。更に、データの無駄を省く為全体のサイズは受信契約情報を暗号化する暗号系におけるブロックサイズと一致させることが望ましい。

【0257】更に、受信契約情報を図50に示すように拡張すると、より多くの契約情報が1つの契約情報パケットで送れることになる。なお、図50では、契約情報パケット中の受信契約情報に関する部分のみを示している。

【0258】図50に示す受信契約情報は、チャンネル契約情報（CHS）を1つしか含まないことを特徴としており、複数ある受信装置ID（TID）は全て、前記チャンネル契約情報を契約内容とする放送受信装置の受信装置IDである。即ち、図49の受信契約情報では1つのチャンネル契約情報と1つ受信装置IDをリンクして記録しているところを、図50では、1つのチャンネル契約情報に複数の受信装置IDをリンクして記録していることが特徴で、これにより契約情報パケットで送れる受信契約情報の量が更に多くなる。

【0259】しかし、問題点もある。例えば、チャンネル契約情報の種類が多くて、対応する契約者が少ないような場合は、図50の形式では空白が多くなってしまい、
50

却って効率が悪くなる。従って、放送受信装置の実装は図49、図50の両方の形式にも対応している課金制御部1106が一般的な意味で望ましい。このためには、両方の形式のバケットを情報識別子で区別し、それに対応した処理部を用意すれば良い。

【0260】受信契約情報に前記認証子を含めると受信契約情報は、図75のような形式になり、前記デジタル署名を含めると受信契約情報は、図76のような形式となる。また、これらに、図49、図50の契約情報バケットの形式を適用することも可能で、その場合はそれぞれ図77、図78のような形式となる。また、当然情報の順序に関しては（受信装置の設計段階で決めておく必要はあるものの）特に制約はなく、図74～図78に示す形式にあっては要素毎に順序を変えたバリエーションは存在する。

【0261】また、これら複数の形式を混在させて送る場合は、図37に示したように、さらに、情報識別子で識別し、それに対応した処理部を用意すれば良い。

【0262】2) 契約管理装置

次に、図31のに示した構成の放送受信装置に対応する、情報配信側の契約管理装置について説明する。

【0263】図70は、本実施形態に係る契約管理装置の構成例を示したもので、本実施形態に示した機能を全て実現したものであり、実現されるシステムにおいて不必要な機能がある場合にはその部分の構成を削ることができる。

【0264】なお、図70において、契約ユーザDB2001、支払い確認待ちDB2002、契約期間確認部2007、契約情報DB2005、スケジューリング部2014、放送装置2013、契約情報バケット出力要請部2012、シードDB2003、シード・マスター鍵生成部2010は、図3の契約管理装置における契約ユーザDB1、支払い確認待ちDB2、契約期間確認部7、付加情報DB5、スケジューリング部14、放送装置13、付加情報出力要請部12、シードDB3、シード・マスターキー生成部10と同様であるので、説明は要略し、本実施形態に特徴的な部分についてのみ説明する。

【0265】なお、図70において、契約変更ユーザDB2006には、所定期間内に契約内容を変更した（新規契約も含まれる）ユーザに関する情報（例えば、受信装置ID、チャンネル番号等のチャンネル契約情報等）が書き込まれるものである。

【0266】図70に示した契約管理装置で特徴的な部分は、契約情報バケット生成部2008である。契約情報バケット生成部2008の構成例を図72に示し、図73に示したフローチャートを参照して、契約情報バケット生成部2008の構成と処理動作について説明する。

【0267】契約情報バケット生成部2008は、契約

管理装置の契約情報バケット制御部2009からの命令を受信契約情報作成部2032で受け、動作を開始する（ステップS1131）。受信契約情報作成部2032に送られる命令としては、例えば、「1998年7月15日に送信予定の最近2ヶ月間に契約変更した契約者の契約情報を順次作成せよ」というような内容である。このような命令を受けた受信契約情報作成部2032では、契約ユーザ情報検索／入力部2031を介して、契約変更ユーザDB2006、場合によっては契約ユーザDB2001を検索し、該当するユーザの情報を順次抽出する（ステップS1132～ステップS1133）。

【0268】次に、チャンネルキー復号鍵検索／入力部2038を介して、チャンネルキー復号鍵DB2016から送信時期に対応したチャンネルキー復号鍵を検索し（ステップS1134）、図74に示すような第1の中間データを生成する（ステップS1135）。

【0269】次に、認証子生成部2036にて、該第1の中間データに対して認証子を作成し（ステップS1136）、それを該第1の中間データに付加して、図75に示すような第2の中間データを作成する。更に、デジタル署名用鍵検索／入力部2037を介してデジタル署名用鍵DB2017から送信時期に対応したデジタル署名用の秘密鍵を検索し、該秘密鍵でデジタル署名を作成し（ステップS1137）、該デジタル署名を第2の中間データに付加して、図76に示すような受信契約情報を作成する（ステップS1138）。

【0270】ここで、デジタル署名の対象とするデータは第1の中間データだけでも良いし、第2の中間データであってもよい。一般に後者の方がより強いセキュリティを実現できる。

【0271】次に、受信契約情報を暗号化部2033に送り、暗号化部2033では、マスター鍵検索／入力部2039を介して、マスター鍵DB2015から放送時期に合ったマスター鍵をマスター鍵DBから検索抽出し（ステップS1139）、それを使って受信契約情報を暗号化する（ステップS1140）。

【0272】契約情報バケット作成部2034では、暗号化された受信契約情報にチャンネルキー復号鍵識別子、マスター鍵識別子、情報識別子を付加して、例えば、図37に示すような契約情報バケットを作成する（ステップS1141）。契約情報バケットを作成するには、図37に示したように、チャンネルキー復号鍵識別子、マスター鍵識別子、情報識別子を付加すれば良いが、前2者はそれぞれのデータベースから取得でき、情報識別子に関しては契約情報バケットに対して予め割りふられた識別子を付加すれば良い。

【0273】また、図49に示すような受信契約情報（もしくは第1の中間データ）を作成することも同様に可能である。更に図50に示すような圧縮された受信契約情報（もしくは第1の中間データ）を作成することも

可能であるが、この場合、契約ユーザ情報検索／入力部2031での処理が複雑になる。即ち、契約ユーザ情報検索／入力部2031は、同じチャンネル契約情報を持った契約者を検索する必要がある。ここで契約の種類が少なければ図50に示すような圧縮された契約情報は有効であるが、契約の種類が多い場合は無駄な領域が増えてしまうので送信量が多くなり不利になる。そこで、図49の形式と図50の形式をチャンネル契約情報に応じて取り混ぜて送る必要もある。この場合どちらの形式にするかを決定するのは受信契約情報作成部2032であり、受信契約情報作成部2032では、契約ユーザ情報検索／入力部2031の検索結果に基づいて決定する。例えば、図49の形式に入るチャンネル契約情報の数が10で、図50の形式に入るチャンネル契約情報の数が20である場合、受信契約情報の作成条件に合う契約者のうち同じチャンネル契約情報を持つ契約者が10件以下であれば図49の形式、11件以上であれば図50の形式とするなどと処理することができる。更に2つの形式の違いをバケット上で明示しなくては、放送受信装置側で処理ができないが、これには情報識別子を利用すれば良い。即ち、契約情報バケットの形式によって複数の情報識別子を使い分けることになる。もちろんこのことは、契約情報バケットが取り得る様々な形式に対して適応することができる。例えばデジタル署名の有無、認証子の有無などは契約情報を図49の形式にするか図50の形式にするかという事柄とは独立であり、どのオプションを取った契約情報バケットであるかを明示することにも情報識別子を利用することができる。

【0274】最後に契約情報の送出スケジュールについて述べる。本発明は、契約情報の送出に使える帯域が狭くて同等の安全性が保証できることが有意点であることから、以下で述べる契約者毎に契約情報の送出頻度を変化させる送信方式は意義が深い。即ち、契約変更者は契約変更の内容にもよるが（特に不利な契約情報の場合は）なるべく受信せずに視聴し続けようとして受信契約情報の受信拒否をすることが考えられる。ここで言う受信拒否は毎日短時間しか視聴しないか、一定期間スイッチをオフにしておく等の単純なものである。

【0275】このような意味からは契約変更後に、契約情報を送る期間を一定なものにすると限定受信が実現できない可能性がある。例えば、契約変更後1年間しか契約情報を送らないとしてしまうと、契約変更後1年間1度も放送受信装置にスイッチを入れないと（契約情報は取得できないので）契約情報が更新されず、それ以降古い契約情報のまま視聴し続けられてしまうことになる。

【0276】一方で契約変更後、受信契約情報を半永久的に送り続けることにすると、既に受信した契約者の分を何度も送信することになるので放送帯域が有効に使えない。そこで、契約変更後の経過時間毎に契約情報の送信頻度を変化させる必要が生じる。契約情報の送信頻度

の一例を以下に示す。

- ・ 契約変更後の経過時間が2ヶ月のとき … 送信頻度は10分に1回
- ・ 契約変更後の経過時間が2ヶ月～6ヶ月のとき … 送信頻度は30分に1回
- ・ 契約変更後の経過時間が6ヶ月～1年のとき … 送信頻度は60分に1回
- ・ 契約変更後の経過時間が1年以上のとき … 送信頻度は120分に1回

10 ここでは、最初の2ヶ月は10分に1回送信し、早期の契約変更を目指す。大多数の受信装置はこの段階で契約変更がなされると考えられるが、たまたま受信できなかったか長期間スイッチをオフしていたため契約情報を受信できなかった受信装置のために、その後も2ヶ月経過後から6ヶ月経過後までに30分に1回、6ヶ月経過後から1年経過後まで60分に1回、1年経過後以降は120分に1回という形で送信頻度を下げて送り続けることにより、放送帯域を節約しながら確実な限定受信を行うことができる。

20 【0277】一方、新規契約者に対しては、契約者自身早期に受信したいと望むし、万が一契約情報が（何らかの原因で）受信できなかった場合でも、後日クレームという形で放送局側にフィードバックがかかるので、このとき再送信すればよく、長期間にわたって送信する意味はあまりない。この意味から新規契約者については、新規契約後2ヶ月間だけ10分に1回程度の頻度で送信すれば足りると考えられる。

【0278】以上のように、契約の種類（例えば、契約変更、新規契約など）と契約後の経過期間によって、契約情報の放送頻度を変更する送信スケジュールが望ましい。本実施形態の契約管理装置にあっては、契約情報バケット生成制御部が例えば上記の頻度で送信するように調整する。

【0279】（第4の実施形態）

1) 放送受信装置

図51は、本実施形態に係る放送受信装置の構成を概略的に示したものである。本実施形態は第3の実施形態と同レベルのセキュリティを保ったまま簡略化したものである。従って、図31と同一部分には同一符号を付し、異なる部分について説明する。

【0280】本実施形態が第3の実施形態と本質的に異なるところは、図31のチャンネルキー復号部1109がないことである。従って、図52に示すように、暗号化された放送コンテンツを復号するための鍵構成が3段になっている。

【0281】また、本実施形態ではチャンネルキーは受信契約情報の中に含まれる。したがって通常チャンネルの情報は、図53に示すように、スクランブルされたコンテンツ情報のみとなる。それに伴い、契約情報チャンネルにて配信される契約情報バケットも図54のようになり、

チャンネルキー復号鍵の代わりにチャンネルキーが入るためチャンネルキー識別子と対応するチャンネル識別子が必要になる。

【0282】受信契約情報は、図55に示したように、受信装置1D、チャンネル契約情報、チャンネルキーから構成される。この受信契約情報も第3の実施形態で述べたように図49に示したのと同様なバッキングが可能である。また、図54に示す契約情報バケットではチャンネル識別子が未暗号化部分にあるため、選択しているチャンネルのチャンネル識別子に対応した契約情報のみを取得することが可能となる。これを避けるため、図57に示すように、受信契約情報中に、チャンネル識別子とチャンネルキー識別子を含めて、これ全体を暗号化する構成を考える。この場合、契約情報バケットは、図56に示すように、暗号化された受信契約情報とマスター鍵識別子と情報識別子を含む構成となる。

【0283】さらに、受信契約情報が図58に示すような構成であるとする、受信契約情報には、チャンネルキー「0」とチャンネルキー「1」が存在し、どちらかが現在の放送コンテンツの復号鍵であり、もう一方が次に有効になる鍵とすることができ、チャンネルキー識別子が要らなくなる。

【0284】更に、第3の実施形態に示した受信契約情報と同様に、受信契約情報に認証子やデジタル署名を付加することができ、付加した場合、第3の実施形態と同様の効果がある。例として最も受信契約情報が複雑になる場合、即ち、図49、図50の形式で受信契約情報を記述し、図58のように2つのチャンネルキーを含めた例を図79、図80にそれぞれ示す。また、情報の順序に関しては第3の実施形態と同様で、特に制約はなく、データ毎に順序を変更することは可能である。また、これら複数の形式を混在させて送る場合は情報識別子で識別すれば良い。

【0285】さて、契約情報受信時は契約情報バケットがフィルター部1107で分離され契約情報復号部1110に送られる。その中に含まれる暗号化された受信契約情報を対応するマスター鍵を用いて復号し、受信契約情報に含まれる受信装置1Dを（複数ある場合は）順次検索して行き、当該受信装置の1Dが見つかった場合は、それに対応するチャンネル契約情報をチャンネル契約情報格納部1116へ格納する。同時に、受信装置1Dが当該受信装置である無しに関わらず、受信契約情報に含まれるチャンネルキーを、該受信契約情報にて示されたチャンネル識別子とチャンネルキー識別子の組合せに対応させて、図59のように、メモリ（図51のチャンネルキー格納部1117）に書き込む。

【0286】チャンネルキー出力部1120はデスクランブル部1108からの要請により契約判定部1118での判定にしたがって、チャンネルキー格納部1117から対応するチャンネルキーを検索して、デスクランブル部1

108に出力する。

【0287】ここでは、図59に示したように、取得した全てチャンネルキーをチャンネル識別子とともにチャンネルキー格納部1117に格納している。しかし、これは同時に視聴するチャンネルは高々1つであるため必ずしも必要はない。そこで認証部1114で現在視聴しているチャンネル番号を参照し、必要なチャンネルキーだけをチャンネルキー格納部1117に格納することも可能である。この場合、チャンネルキー格納部1117には、図41に示したように、チャンネルキーとその識別子とが格納される。この構造を取った場合、チャンネル変更時にはチャンネルキー格納部1117の内部をクリアしなくてはならない。何故なら変更後のチャンネルのチャンネルキーは変更前のチャンネルのチャンネルキーとは一般的に異なるので、格納部をクリアしないと変更前のチャンネルのチャンネルキーが有効になってしまい、意味不明の放送コンテンツが出力されることになるからである。このようにすることによって、チャンネル変更時には、チャンネルキー格納部1117をクリアしてチャンネル契約情報から新たにチャンネルキーを取得しなくてはならないため、デスクランブルまでに処理時間がかかるが、チャンネルキー格納部1117のメモリ容量が少なくても済み、また、チャンネル数が増えてもメモリ容量を増やすなどの処置をしなくても良い。

【0288】このような方式を実現するためには、認証部1114がチャンネル情報入力部1119からチャンネル番号を取得する必要がある、図51の点線で示したようなデータの流れが更に必要である。

【0289】また、本実施形態の方式を取ることににより、第3の実施形態と比較して鍵構成を1段減らせることによるメリット以外にも、次のようなメリットがある。すなわち、全チャンネルを1ヶ月分契約した契約者が次の月に全てのチャンネルを解約したとする。この場合、この契約者は自分の放送受信装置宛の新しい受信契約情報を取得したくない。何故なら取得すると全チャンネルが視聴できなくなってしまうからである。しかし、受信契約情報の中には放送コンテンツの復号のために必要な情報があるのでその全てを取得しない訳にはいかない。第3の実施形態の場合は、必要な情報はチャンネルキー復号鍵 K_H であった訳であるが、これは全チャンネルに対して共通であるのでチャンネルキー復号鍵 K_H が変更されるタイミングに対し、高々1つの受信契約情報を取得すれば良い。もし、 K_H の変更が1日に1回であれば、自分の放送受信装置宛での受信契約情報を受け取らないことも十分に可能である。これに対して、本実施形態では必要な情報はチャンネルキーそのものであり、しかもチャンネルキーはチャンネル毎に異なり、安全性の必要上頻繁に変更する必要がある。このため、受信契約情報もかなり頻繁に取得する必要性に迫られ、自分の放送受信装置宛での受信契約情報を受け取らない確率はかなり低くなる。

【0290】だが、第3の実施形態の4段の鍵構成にも積極的に採用するに足る意義がある。もし、チャンネルが多く（例えば1000チャンネル）あった場合、受信開始時もしくはチャンネル変更時にかなりの数（最悪1000個）の受信契約情報を取得して復号した後でない、当該チャンネルのチャンネルキーは取得できない。これでは受信のタイミングがかなり遅くなって実用に耐えないばかりか、万一受信誤りが生じた場合がもう1000個復号するまで待たなくてはならない。この点を解消したのが4段の鍵構成である。

【0291】4段の鍵構成の場合、チャンネルキー復号鍵という全ての放送受信装置に共通の鍵があり、全てのチャンネルキーがそれで復号されるためチャンネルの数に依らず一定の時間で復号できる。これらの利点を生かして、構成された放送受信装置の構成例を図60に示す。ここでは、契約情報パケットおよび受信契約情報のフォーマットを2種類用意し、1つは第3の実施形態で示した図37、図38のようなものであり、他の1つは本実施形態に係る図54、図55のようなものである。

【0292】これらの違いを契約情報パケット中の情報識別子で判断し、認証部1114では、受信契約情報に含まれているものがチャンネルキー復号鍵であれば、チャンネルキー復号鍵格納部1115へ、チャンネルキーであればチャンネルキー格納部1117へ送る。

【0293】なお、受信契約情報にチャンネルキー復号鍵が含まれる時には、通常チャンネルにて別途チャンネルキー情報を送り、そうでない時にはチャンネルキー情報を送らないように放送局（契約管理装置）側で調整する。このため両方の回路が混在しても矛盾なく動作することができる。

【0294】2）契約管理装置

次に、本実施形態に係る放送受信装置に対応する、情報配信側の契約管理装置について説明する。

【0295】図71は、本実施形態に係る契約管理装置の構成例を示したもので、本実施形態に示した機能を全て実現したものであり、実現されるシステムにおいて不必要な機能がある場合にはその部分の構成を削ることができる。なお、図71に示した契約管理装置において、図70に示した第3の実施形態における契約管理装置と同一部分には、同一符号を付し、異なる部分について説明する。すなわち、図70のチャンネルキー復号鍵DB2016とチャンネルキー復号鍵生成部2018が図71では、それぞれ、チャンネルキーDB2021、チャンネルキー生成部2022に置き換えられ、図71のチャンネルキーDB2021、チャンネルキー生成部2022の処理動作の説明は、図70のチャンネルキー復号鍵DB2016とチャンネルキー復号鍵生成部2018の説明部分において、チャンネルキー復号鍵をチャンネルキーと置き換えれば、同様である。

【0296】（第5の実施形態）第5の実施形態では、

第1～第4の実施形態の限定受信システムに共通に利用可能で、放送受信装置内にある課金制御部1106のテスト用ラッチ部の構成に関する実施形態を示すものである。図61に、本実施形態に係る放送受信装置の構成例を示す。

【0297】受信限定システムは、その構成上、課金制御部1106の内部の秘密情報（特にマスター鍵生成の鍵やアルゴリズム）が露見すると、システム全体が破綻し、有効な課金ができなくなる危険がある。また、例えば図31において出力されたデスクランブルされた放送コンテンツが何らかの手段でユーザに記録されるとそれを何回でも再生することが原理的にできてしまい好ましくない。その意味から課金制御部1106とその出力を利用するMPEGデコーダは一体化されたチップで構成されていることが好ましい。

【0298】一方、一体化されたチップを作成する際は1回で正しいチップを作成することは困難なので中間結果をテストピンなどを通して見てみる必要がある。また、このテストピンは製品段階でも残ってしまうので、本チップを解析しようとする者に対して復号プロセスを中間結果といえども観察できる機会を与え、暗号アルゴリズムや復号鍵の解析に都合の良い状況を作り出してしまう。そこで考えられたのが本実施形態である。

【0299】上記目的を達成するために、第1～4の実施形態に示した放送受信装置に付加するものは、図61に示すように、スキャンバステスト用ラッチ部1201、1203と、スキャンバス出力部1202、1204である。

【0300】スキャンバステスト用ラッチ部1201、1203は、そこを流れるデータを捕え、それぞれスキャンバス出力部1202、1204へ送る動作を行う。

【0301】1）スキャンバステスト用第1のラッチ部（受信契約情報のテスト出力）

図62に、スキャンバステスト用第1のラッチ部1201の基本的な構成例を示し、図63に示すフローチャートを参照しながらスキャンバステスト用第1のラッチ部1201の構成およびその処理動作について説明する。

【0302】スキャンバステスト用第1のラッチ部1201では、契約情報復号部1110からの出力（復号された受信契約情報）を入力部1301で受取り（ステップS1101）、そのデータを（必要があれば）データフォーマットの変更などを行い認証部1302へ送る。認証部1302では、当該情報を出力しても良いか否かの判定を行う（ステップS1102）。もし、出力しても良いと判定された場合、当該データを出力部1305へ送り（ステップS1103）、出力部1305は、第1のスキャンバス出力部1202へ送る（ステップS1104）。第1のスキャンバス出力部1202は、当該データを課金制御部1106外へ出力し、当該データは課金制御部1106外にあるディスプレイ装置等の表示

部に表示される(ステップS1105)。

【0303】認証部1302にて、ステップS1105の処理に続いて、あるいは、復号された受信契約情報を出力しないと判定したとき、当該復号された受信契約情報をそのままスキャンバステスト用第1のラッチ部1201の外部にある認証部1114へ出力する(ステップS1106)。

【0304】ここで、認証部1302の働きは重要である。以下では認証部1302の働きを説明するため、課金制御部1106への入力データフォーマットに立ち戻って説明する。まず簡単のため最も単純な実現方法を示す。第3、第4の実施形態における契約情報パケットの構成(図37、図54参照)にある情報識別子として、通常の(受信契約情報を示す)識別子以外にスキャンバス出力が可である受信契約情報である旨を示す識別子を設ける。この情報識別子を認証部1302で判断することによって当該データを第1のスキャンバス出力部1202に出力するか否かを決定するのである。

【0305】スキャンバス出力をさせる必要があるのは、基本的に設計時もしくは工場出荷時であるので、スキャンバス出力を可にする情報識別子は放送波では流さないと考えて良く、当該情報識別子がどのようなものを一般のユーザが解析するのは困難である。

【0306】次に、スキャンバス出力が可である受信契約情報を含む契約情報パケットであるか否かを、契約情報パケットに対応した認証情報で判定する例を示す。この場合の契約情報復号部1110へ入力する契約情報パケットのフォーマットを図64に示す。

【0307】図37と異なるのは、暗号化された受信契約情報に続いて認証情報がさらに加わった点である。勿論、図54の場合も図64と同様に変更すればよい。なお、(認証情報がない)通常のフォーマットの契約情報パケットと区別するために、そのための情報認証子を別に設定するか、情報識別子を共通にした場合は、フォーマットをそろえるため、通常の契約情報パケットにおける認証情報は「NULL」として、「NULL」の認証情報パケットが来た場合は通常の契約情報パケットであると解釈しても良い。但し、後者の場合は実装が簡単だが、データ量が多くなるという欠点がある。

【0308】認証情報として、例えば暗号化された受信契約情報(もしくはそのハッシュ値)に電子署名を施したものを考える。ここでデータのハッシュ値とは任意長のデータを一定の長さ(例えば120ビット)で表現したデータのダイジェストのようなものである。ダイジェストといっても内容そのものの要約ではなく、データにハッシュ値と呼ばれる何らかの方向性関数(逆関数を求めることが困難な数学的関数)を施して、一定の長さにしたものと言うことができる。このようなハッシュ関数はMD5やSHA1などいくつか知られている。電子署名を付けるデータは暗号の1ブロックにあたる64ビ

ットもしくは120ビットの一定の長さしておく必要がある。このため必要があれば受信契約情報にハッシュ関数を掛ける。

【0309】スキャンバステスト用第1のラッチ部1201が、復号された受信契約情報とともに、認証情報と暗号化された受信契約情報も受取り、認証情報としての電子署名を確認する、確認のプロセスを含めたスキャンバステスト用第1のラッチ部1201の処理動作について、図66に示すフローチャートを参照しながら説明する。

【0310】入力部1301には、復号された受信契約情報とともに、認証情報と暗号化された受信契約情報も受取り(ステップS1121)、認証部1302では、電子署名の確認のためにはまず(入力された)暗号化された受信契約情報に(必要に応じて)ハッシュ関数を掛ける(ステップS1122)。一方、認証部1302に予め格納されている公開鍵で認証情報としての電子署名を復号し(ステップS1123)、前記ハッシュ値と比較する。ここで一致していれば(ステップS1124)、認証情報は正しいと考えることができ、図63のステップS1103～ステップS1105と同様にし、データの出力を行う(ステップS1125～ステップS1127)。

【0311】ステップS1124で、一致していなければ、当該認証情報は正しくないと判定して、データの出力は行わない(ステップS1128)。ステップS1127の処理に続いて、あるいは、認証情報とハッシュ値とが一致しないとき、当該復号された受信契約情報をそのまま、スキャンバステスト用第1のラッチ部1201の外部にある認証部1114へ出力する(ステップS1128)。

【0312】ここで、公開鍵暗号を使った電子署名はデータ本体(ここではハッシュ値)に対して秘密鍵で暗号化したものを言う。公開鍵暗号において秘密鍵で暗号化したものは公開鍵といわれる秘密鍵とは別の鍵でなくては復号できない。このため電子署名を公開鍵で復号すれば元のハッシュ値になるはずである。また、公開鍵暗号の安全性から公開鍵で復号できるようなデータを作成できるのは秘密鍵を知っている人だけと考えられるので、ハッシュ値を秘密鍵で暗号化したデータを当該データの電子署名と呼んでいる。ここで公開鍵暗号を使った電子署名を使う意義は、課金制御部1106内の情報だけでは電子署名を作成できないので一般者がスキャンバステスト用ラッチ部1201、1203に対して出力させるようなデータを作成するのは事実上不可能である点である。また、電子署名は共通鍵暗号を使っても可能となる。この場合ハッシュ値を共通鍵で暗号化し、共通鍵で復号することによって確認するので、共通鍵は当該ラッチ部に秘匿しておかなくてはならない。しかし、共通鍵暗号は公開鍵暗号に比べて高速であるという特徴があ

り、このための共通鍵は課金チップという耐タンパはハードウェア上に隠されているので、読み取るのは極めて困難である。このことから共通鍵による電子署名も有効である。

【0313】暗号化された電子署名を確認するため、スキャンバステスト用第1のラッチ部1201には、本来必要のない暗号化された受信契約情報を入力している。これを避けるためには契約情報復号部1110で電子署名を検証し、その結果をスキャンバステスト用第1のラッチ部1201に送るという方法が考えられる。即ち、スキャンバステスト用第1のラッチ部1201の認証部1302の主要部分を契約情報復号部1201で行なうという訳である。だが、この方法ではラッチ部に対して出力を促すデータは常に同じであり、第3者による悪用を許しやすい。

【0314】その意味で契約情報復号部1110で署名が認証された場合、契約情報復号部1110でその出力に電子署名を施すという実現方法もある。この方法によれば前記の悪用の問題は避けられるが、処理が余分にかかる。いずれの方法を取るかはアプリケーションの性質によって決まる。

【0315】次にスキャンバステスト用第1のラッチ部1201が出力するデータについて考えてみると、前記の全ての例では生のデータ列(0、1の列)、すなわち、復号された契約受信情報そのものが出力される。もしデータ列が暗号化されていれば、更に安心である。即ち、例えばスキャンバステスト用第1のラッチ部1201から無条件でデータが出力されてもそのデータが暗号化されており、復号鍵を備えた表示装置でないと復号できないような構成にしていれば当該ラッチ部1201の出力から課金制御部1106の構成を解析することは極めて困難である。

【0316】このようなスキャンバステスト用第1のラッチ部1201の構成例を図66に示す。図66において、暗号化部1303に公開鍵暗号を導入して、公開鍵で暗号化するようにすれば更に安全である。何故なら暗号化された出力データは課金制御部1106内には含まれない秘密鍵でしか復号できないからである。しかし、実際は処理時間の観点で共通鍵暗号を使われる機会が多いだろう。この場合共通鍵を暗号化鍵格納部1304に秘匿しておく必要がある。さもないと、せっかく暗号化しても第三者に共通鍵が露見すれば復号されて、出力内容が露見してしまうからである。

【0317】2) スキャンバステスト用第2のラッチ部(受信装置IDのテスト出力)

次に、図61のスキャンバステスト用第2のラッチ部1203について説明する。スキャンバステスト用第2のラッチ部1203の動作も前述の第1のラッチ部1201と基本的には同じであるが、第1のラッチ部1201がいわばデータが一方向に通るだけであったのに

対し、第2のラッチ部1203は受信装置ID格納部1113から受信装置IDの読み込みを行い、その結果をラッチするのであるから構成が多少複雑になる。

【0318】この第2のラッチ部1203は、受信装置IDが、例えば、不揮発性メモリにて構成されている受信装置ID格納部1113に正しく格納されているかを確認するためのものである。

【0319】図67にスキャンバステスト用第2のラッチ部1203の構成例を示す。

【0320】認証部1114からのデータは、スキャンバステスト用第2のラッチ部1203の第1の入力部1401で受取り、認証部1402へ送られる。認証部1402は、前述の第1のラッチ部1201の認証部1302と同様に、入力結果に対するラッチ出力の可否に関する認証を行う。

【0321】認証結果は認証結果格納部1403に格納される。一方、認証部1402から受信装置ID格納部1113へは、受信装置IDの出力を要請する命令を流す。それを受け取った受信装置ID格納部1113は、受信装置IDを出力し、第2の入力部1405へそれを入力する。受信装置IDはラッチ出力可否判定部1404へ送られ、ラッチ出力可否判定部1404では、認証結果格納部1403にある認証結果を参照して、認証されている場合には、受信装置IDを第2のスキャンバス1204へ出力する。

【0322】なお、ラッチ出力可否判定部1404は、認証部1402で認証されている場合でもされていない場合でも、受信装置ID格納部1113から受け取った受信装置IDは外部の認証部1114へ出力する。

【0323】また、ラッチ出力可否判定部1404の後段に、図66に示したような暗号化部1303、暗号鍵格納部1304を付け加えれば、前述同様、受信装置IDを暗号化して出力することもできる。

【0324】(第6の実施形態)

1) 放送システムの概略

放送受信装置に受信契約情報を放送配信する以外に、磁気カード等の形態可能な記録媒体(以下、簡単にカードPと呼ぶ)に記録し、それを当該放送受信装置に宅配又は郵送する点が、前述の第3～第5の実施形態の場合と異なる。契約ユーザは、放送受信装置に受け取ったカードPに記録された情報を読み取らせることにより、契約チャンネルの受信が可能となる。

【0325】ここでは、第3の実施形態の契約管理装置(図70参照)、放送受信装置(図31)に対応した契約管理装置(図81参照)、放送受信装置(図82参照)を例にとり説明するが、他の実施形態に係る契約管理装置、放送受信装置も、基本的には同様である。すなわち、第6の実施形態に係る契約管理装置では、第3～第5の実施形態に係る契約管理装置の放送装置2013がカード作成部2051に置き換えられ、あるいは、さ

らに追加されている。カード作成部2051は、契約ユーザのカードPに暗号化された受信契約情報を書き込むようになっている。また、第6の実施形態に係る放送受信装置では、契約情報復号部1110に、カードリーダー2061に挿入されたカードPから読み取られた暗号化された受信契約情報が入力するようになっている。

【0326】2) 契約管理装置

図81は、第6の実施形態に係る契約管理装置の構成例を示したもので、図70と同一部分は同一符号を付し、異なる部分について説明する。すなわち、図70の受信装置毎の受信契約情報を地上波あるいは衛星放送を介して配信するための放送装置2013が図81では、カード作成部2051に置き換えられ、あるいは、さらに追加して必要に応じて適宜切り替えられるようになっている。

【0327】カード作成部2051により、カードPに、そのカードPに対応した受信装置の契約期間に応じた受信契約情報等を記録して、契約ユーザに配布するようになっている。

【0328】例えば、1997年12月1日から4ヶ月間契約している契約ユーザに対しては、マスターキーが1ヶ月毎に更新されるとき、受信契約を1ヶ月毎に作成しなくてはならないために1ヶ月毎に有効なチャンネルキー復号鍵と有効なマスターキーを検索して、図73のフローチャートに示す処理を行う必要がある。図81に示す契約管理装置では、受信契約情報を放送によらずに例えばカードPに4ヶ月分の契約チャンネルのチャンネルキー復号鍵に対応する受信契約情報を書込み、当該ユーザに配送すればよい。これにより、1ヶ月毎の配信、配布を行わなくてもよく、放送局側にもユーザ側にも煩雑を避ける意味で有利である。

【0329】ところで、受信契約情報を作成するためには、契約管理装置は、契約ユーザの購入した放送受信装置の受信装置IDを知る必要がある。もちろん、この受信装置IDは、各放送受信装置内の耐タンパな受信装置ID格納部1113に書き込まれているため、外部からの読取りは不可能である。従って、契約管理装置に契約ユーザの購入した放送受信装置の受信装置IDを入力するための手段が必要になってくるであろう。

【0330】そこで、次に、契約管理装置に、購入された放送受信装置の受信装置IDを入力するための一手段を説明する。

【0331】例えば、購入された放送受信装置の筐体や包装用のパッケージ等に当該放送受信装置の表層受信装置ID（受信装置IDに1対1に対応するような識別子で、例えば、受信装置IDそのものを暗号化したものであってもよい）を印刷する。図81に示したように、契約管理装置に入力部2072、表層受信装置ID変換部2071を新たに設ける。

【0332】契約情報入力部2072からは、契約時、

ユーザの契約情報と当該ユーザの購入した放送受信装置の表層受信装置IDを入力するものとする。この入力には、例えば、スキャナ等を用いてもよく、特に限定しない。

【0333】表層受信装置ID変換部2071には、予め、表層受信装置IDと受信装置IDとの対応関係を示した変換テーブル2073を記憶している。

【0334】契約情報入力部2072に入力された表層受信装置IDは、表層受信装置ID変換部2071に渡され、ここで、変換テーブル2073を参照して、表層受信装置IDから受信装置IDへ変換し（すなわち、変換テーブル2073から表層受信装置IDに対応する受信装置IDを検索する）、その結果得られた受信装置IDを支払確認待ちDB2002に渡す。

【0335】一方、契約情報入力部2072に入力された契約情報は、支払確認待ちDB2002に渡される。支払確認待ちDB2002は、当該契約情報を、表層受信装置ID変換部2071から受け取った受信装置IDに対応させて登録する。

【0336】その後の支払確認待ちDB2002に対する処理動作は、図3の支払確認待ちDB2と同様である。

【0337】2) 受信装置

図82は、第6の実施形態に係る放送受信装置の構成例を示したものである。なお、図31と同一部分には同一符号を付し、異なる部分について説明する。すなわち、前述の図81に示したような放送局側に設置されている契約管理装置で作成されたカードPから暗号化された受信契約情報を読み取るためのカードリーダー2061がさらに追加されて、カードリーダー2061にてカードPから読み取られた暗号化された受信契約情報は、契約情報復号部1110に入力される。

【0338】なお、その後の動作は、第3の実施形態と同様である。

【0339】

【発明の効果】以上説明したように、本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信が実現できる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態（付加情報を放送配信する場合）に係る契約管理装置および放送受信装置を用いた放送システムの概略構成を示した図。

【図2】図1に示した放送サービスへの加入・継続契約時、契約更新時、解約時、課金手続きの概略的に流れを示した図。

【図3】第1の本実施形態に係る契約管理装置の構成例を示した図。

【図4】契約管理装置の契約ユーザDBのデータ記憶形

式の一例を示した図。

【図 5】契約管理装置のシード DB のデータ記憶形式の一例を示した図。

【図 6】契約管理装置のチャンネル DB のデータ記憶形式の一例を示した図。

【図 7】契約ユーザへ登録処理を説明するためのフローチャート。

【図 8】契約管理装置の処理動作（契約ユーザ毎に対応した付加情報を生成し、これを配信するまでの手順）を説明するためのフローチャート。

【図 9】（a）図は主にコンテンツを配信するための放送波に多重される情報の一例を概念的に示した図で、（b）図は付加情報のデータ形式の一例を示した図。

【図 10】コンテンツ情報の配信装置の構成例を示した図。

【図 11】（a）図は主にコンテンツを配信するための放送波に多重される情報の他の例を概念的に示した図で、（b）図は付加情報のデータ形式の他の例を示した図。

【図 12】端末付加情報のデータ形式の一例を示した図。

【図 13】チャンネル付加情報のデータ形式の一例を示した図。

【図 14】第 1 の実施形態に係る受信装置の構成例を示した図。

【図 15】図 14 の受信装置の処理動作を説明するためのフローチャート。

【図 16】図 14 の受信装置の処理動作を説明するためのフローチャート。

【図 17】図 14 の受信装置の処理動作を説明するためのフローチャート。

【図 18】図 14 の受信装置の処理動作を説明するためのフローチャート。

【図 19】新規契約に関する付加情報（ON 信号）の送信量と、解約に関する付加情報（OFF 信号）の送信量の時間経過に伴う変動を示した図。

【図 20】付加情報の受信状況を監視する処理を伴う場合の受信装置のフィルタの処理動作を説明するためのフローチャート。

【図 21】端末付加情報とチャンネル付加情報とを用いた場合の図 14 の受信装置の処理動作を説明するためのフローチャート。

【図 22】端末付加情報とチャンネル付加情報とを用いた場合の図 14 の受信装置の処理動作を説明するためのフローチャート。

【図 23】端末付加情報とチャンネル付加情報とを用いた場合の図 14 の受信装置の処理動作を説明するためのフローチャート。

【図 24】本発明の第 2 の実施形態（付加情報をカード型記録媒体に記録して顧客に配布する場合）に係る放送

システムの概略構成を示した図。

【図 25】第 2 の実施形態に係る契約管理装置の構成例を示した図。

【図 26】第 2 の実施形態に係る受信装置の構成例を示した図。

【図 27】カード型記録媒体に記録される付加情報の一例を示したもので、（a）図はマスターキー Km とチャンネルサブキー H の更新時期が同じ場合で、（b）図はマスターキー Km の更新時期が例えば 2 ヶ月毎であるのに対し、チャンネルサブキー H の更新時期が 1 ヶ月毎である場合を示している。

【図 28】図 26 の受信装置の処理動作を説明するためのフローチャート。

【図 29】図 26 の受信装置の処理動作を説明するためのフローチャート。

【図 30】図 26 の受信装置の処理動作を説明するためのフローチャート。

【図 31】本発明の第 3 の実施形態に係る放送受信装置の構成例を示した図。

【図 32】第 3 の実施形態の放送コンテンツの暗号化に用いる 4 段の鍵構成を説明するための図。

【図 33】通常チャンネルによる配信構造の一例を示した図。

【図 34】通常チャンネルにて配信される放送コンテンツ情報の構造の一例を示した図。

【図 35】通常チャンネルにて配信されるチャンネルキー情報の構造の一例を示した図。

【図 36】契約情報チャンネルの配信構造の一例を示した図。

【図 37】契約情報チャンネルにて配信される契約情報バケットの構造の一例を示した図。

【図 38】契約情報バケットに含まれる受信契約情報の構造の一例を示した図。

【図 39】契約情報チャンネルにて配信されるマスター鍵シード情報の構造の一例を示した図。

【図 40】チャンネルキー切替え時点でチャンネルキー「0」とチャンネルキー「1」の送信がオーバーラップする時間帯（Tx 1、Tx 2）が存在する様子を説明するための図。

【図 41】チャンネルキー格納部 1117 におけるチャンネルキーとその識別子との格納形態の一例を示した図。

【図 42】放送受信装置の処理動作を説明するためのフローチャート。

【図 43】放送受信装置の処理動作のうち、放送コンテンツに対する処理動作を示したフローチャート。

【図 44】放送受信装置の処理動作のうち、チャンネルキー情報に対する処理動作を示したフローチャート。

【図 45】放送受信装置の処理動作のうち、契約情報バケットに対する処理動作を示したフローチャート。

【図 46】暗号化された鍵情報に対する認証子について

説明するための図。

【図 4 7】暗号化されない鍵情報に対する認証子について説明するための図。

【図 4 8】暗号化されない鍵情報に対する認証子について説明するための図。

【図 4 9】複数の放送受信装置の受信契約情報を圧縮して送信する場合の送信形態の一例を示した図。

【図 5 0】複数の放送受信装置の受信契約情報を圧縮して送信する場合の送信形態の他の例を示した図。

【図 5 1】本発明の第 4 の実施形態に係る放送受信装置 10 の構成例を示した図。

【図 5 2】第 4 の実施形態の放送コンテンツの暗号化に用いる 3 段の鍵構成を説明するための図。

【図 5 3】通常チャンネルによる配信構造の一例を示した図。

【図 5 4】契約情報チャンネルにて配信される契約情報バケットの構造の一例を示した図。

【図 5 5】受信契約情報の構造の一例を示した図。

【図 5 6】契約情報バケットの構造の一例を示した図。

【図 5 7】受信契約情報の構造の他の例を示した図。

【図 5 8】受信契約情報の構造のさらに他の例を示した図。

【図 5 9】図 5 1 のチャンネルキー格納部における信契約情報にて示されたチャンネル識別子とチャンネルキー識別子の格納形式の一例を示した図。

【図 6 0】受信契約情報中にチャンネルキー復号鍵が含まれる場合とチャンネルキーが含まれる場合とを受信契約情報に付加された情報識別子にて区別して、処理を切り替える放送受信装置の構成例を示した図。

【図 6 1】本発明の第 5 の実施形態に係る放送受信装置 30 の構成例を示した図。

【図 6 2】スキャンバステスト用第 1 のラッチ部の基本的な構成例を示した図。

【図 6 3】図 6 2 のスキャンバステスト用第 1 のラッチ部の処理動作を説明するためのフローチャート。

【図 6 4】スキャンバス出力が可である受信契約情報を含む契約情報バケットであるか否かを判定するための認証情報を含む契約情報バケットの一例を示した図。

【図 6 5】図 6 2 のスキャンバステスト用第 1 のラッチ部の他の処理動作を説明するためのフローチャートで、 40 認証情報として電子署名を用いた場合を示したものである。

【図 6 6】スキャンバステスト用第 1 のラッチ部の他の構成例を示した図で、出力する内部データ（受信契約情報）を暗号化して出力するための構成部を追加したものである。

【図 6 7】スキャンバステスト用第 2 のラッチ部の構成例を示した図。

【図 6 8】受信契約情報にデジタル署名が含まれる場合の放送受信装置の認証部 1 1 1 4 の構成例を示した図。 50

【図 6 9】デジタル署名が含まれている場合の受信契約情報の構造例を示した図。

【図 7 0】第 3 の実施形態に係る契約管理装置の構成例を示した図。

【図 7 1】第 4 の実施形態に係る契約管理装置の構成例を示した図。

【図 7 2】契約管理装置の契約情報バケット生成部の構成例を示した図。

【図 7 3】契約情報バケット生成部の処理動作を説明するためのフローチャート。

【図 7 4】第 3 の実施形態で用いる受信契約情報の基本的な構成例を示した図。

【図 7 5】復号の際の誤り検出に用いる認証子を含む受信契約情報の構成を示した図。

【図 7 6】復号の際の誤り検出に用いる認証子とデジタル署名とを含む受信契約情報の構成を示した図。

【図 7 7】受信契約情報に認証子とデジタル署名を含む場合の契約情報バケットの送信形態の一例を示した図。

【図 7 8】受信契約情報に認証子とデジタル署名を含む場合の契約情報バケットの送信形態の他の例を示した図。

【図 7 9】第 4 の実施形態に係る複数の放送受信装置の受信契約情報（チャンネルキーが 2 つある場合）を圧縮して送信する場合の送信形態の一例を示した図。

【図 8 0】第 4 の実施形態に係る複数の放送受信装置の受信契約情報（チャンネルキーが 2 つある場合）を圧縮して送信する場合の送信形態の他の例を示した図。

【図 8 1】カードに受信契約情報を書き込んで配布する契約管理装置の構成例を示した図。

【図 8 2】配布されたカードから受信契約情報を読み取る放送受信装置の構成例を示した図。

【符号の説明】

契約管理装置

1 … 契約ユーザデータベース

2 … 支払い確認待ちデータベース

3 … シードデータベース

4 … チャンネルキーデータベース

5 … 付加情報データベース

6 … 契約解除ユーザデータベース

7 … 契約期間確認部

8 … 付加情報生成部

9 … 付加情報生成制御部

1 0 … シード・マスターキー生成部

1 1 … チャンネルキー生成部

1 2 … 付加情報出力要請部

1 3 … 放送装置

1 4 … スケジューリング部

1 5 … カード作成部

2 0 0 8 … 契約情報バケット生成部

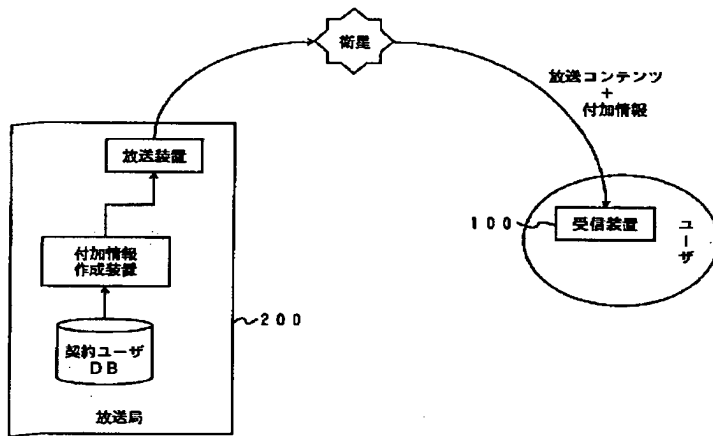
2 0 0 9 … 契約情報バケット生成制御部

2051…カード作成部
 放送受信装置
 501…受信部
 502…A/D変換部
 503…フィルタ
 504…マスターキー生成部
 505…マスターキー格納部
 506…ID格納部
 507…判定部
 508…チャンネルサブキー格納部
 509…チャンネルデコーダ
 510…D/A変換部
 511…再生部
 512…付加情報格納部

*513…カードリーダー
 1106…課金制御部
 1109…チャンネルキー復号部
 1110…契約情報復号部
 1111…マスター鍵格納部
 1114…認証部
 1118…契約判定部
 1120…チャンネルキー出力部
 1201…スキャンバステスト用第1のラッチ部
 1202…第1のスキャンバス出力部
 1203…スキャンバステスト用第2のラッチ部
 1204…第2のスキャンバス出力部
 2061…カードリーダー

*

【図1】



【図4】

契約ユーザDB

受信端末ID	チャンネル番号	契約期間
--------	---------	------

【図6】

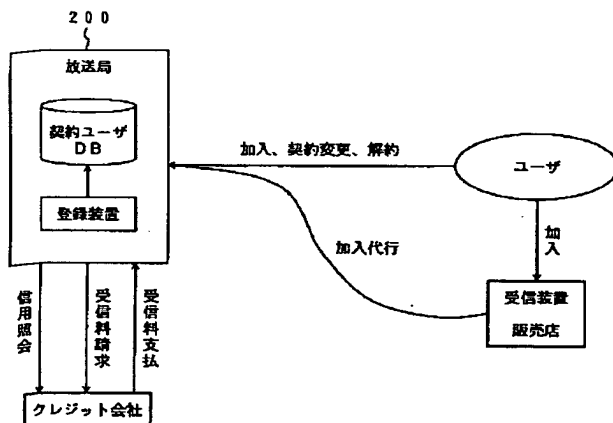
チャンネルキーDB

チャンネル番号	チャンネルキーID	チャンネルキー	有効期間
---------	-----------	---------	------

【図41】

チャンネルキー	0
チャンネルキー	1

【図2】

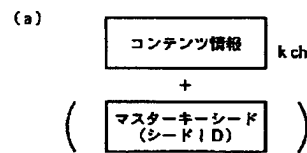


【図5】

シードDB

シードID	マスターキー	有効期間
-------	--------	------

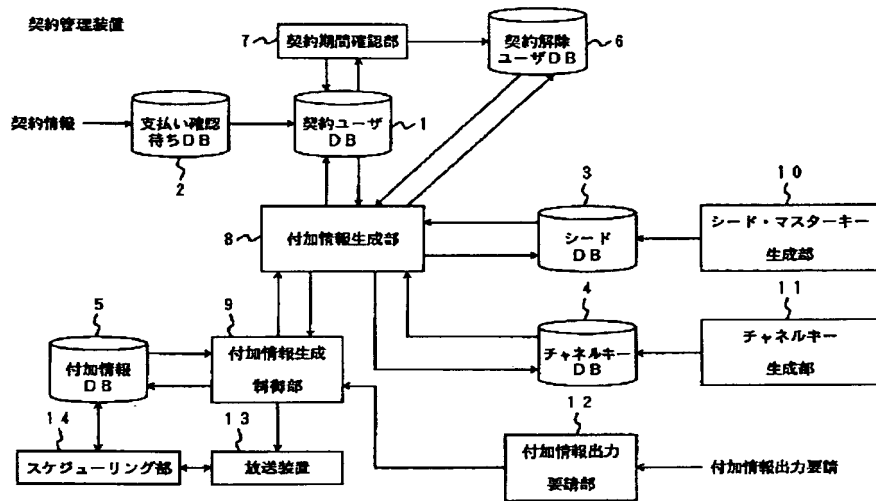
【図9】



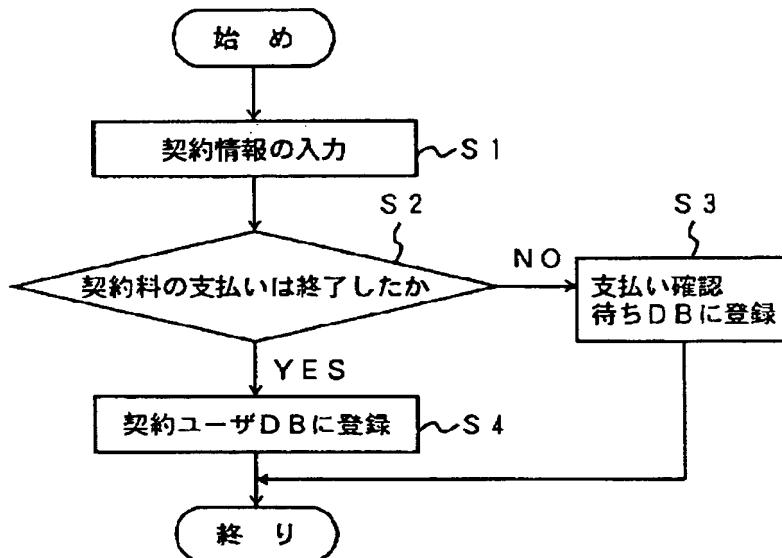
(b)

端末ID	チャンネルキーkch	チャンネル番号	km
------	------------	---------	----

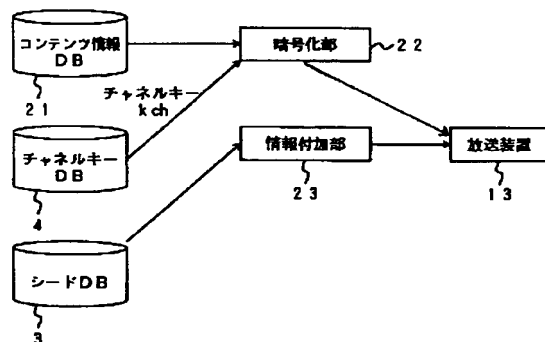
【図3】



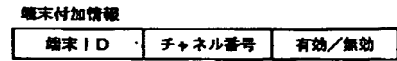
【図7】



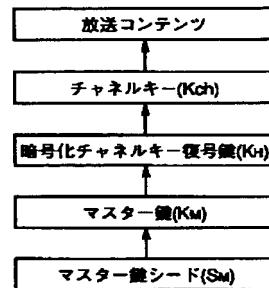
【図10】



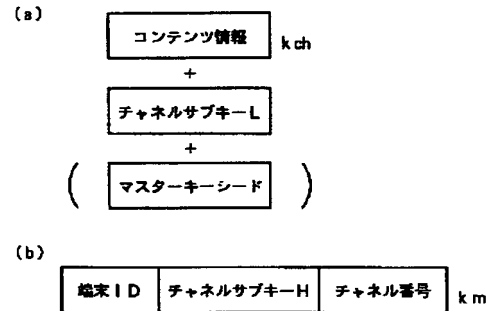
【図12】



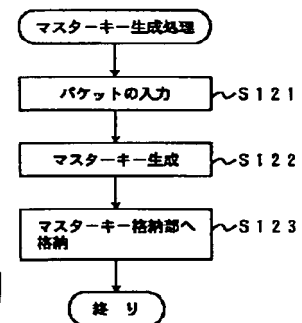
【図32】



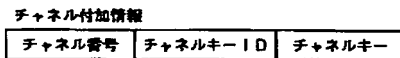
【図11】



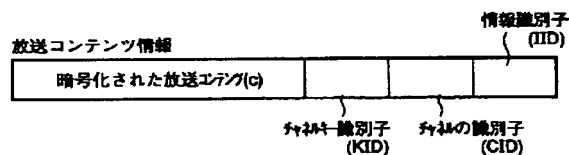
【図16】



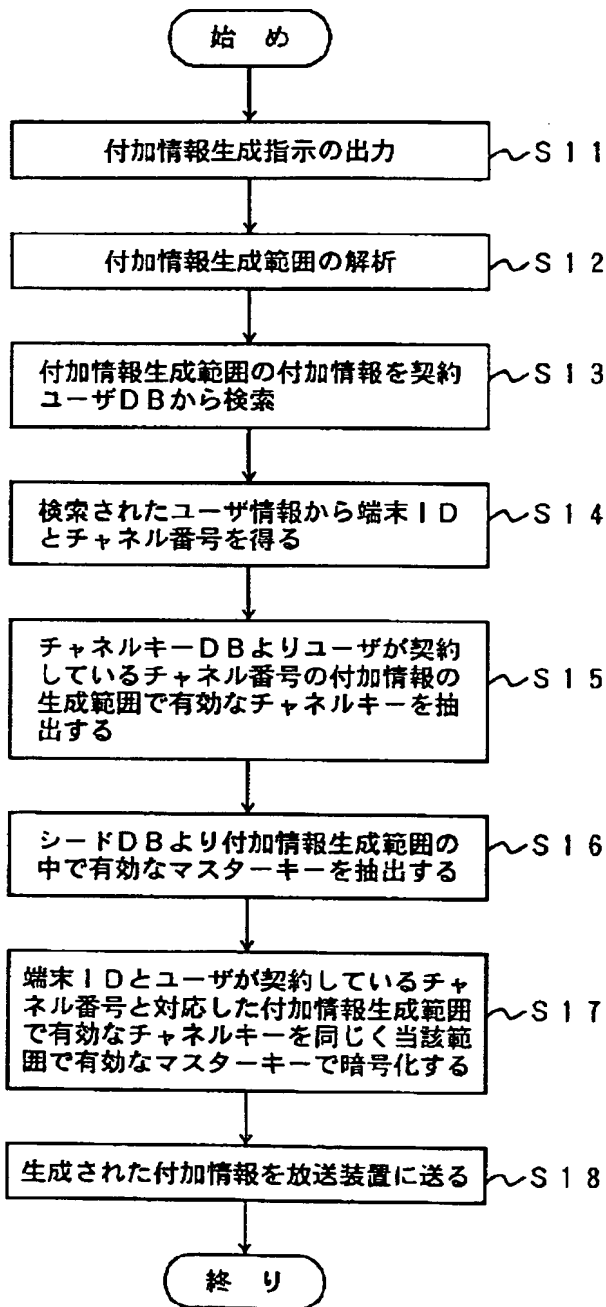
【図13】



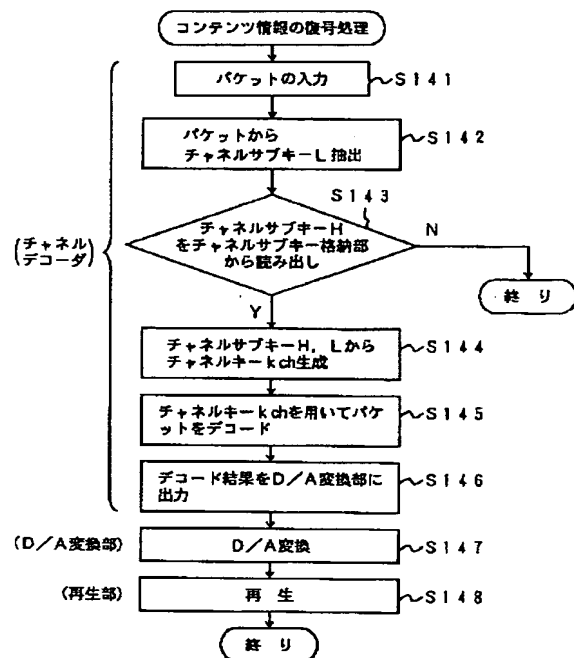
【図34】



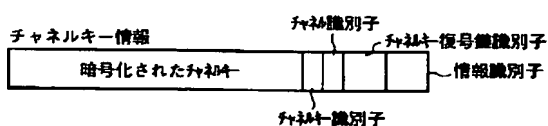
【図8】



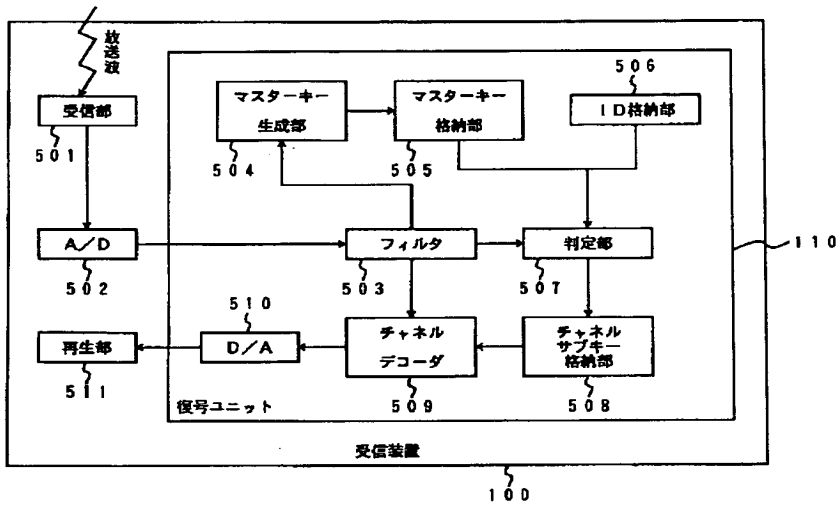
【図18】



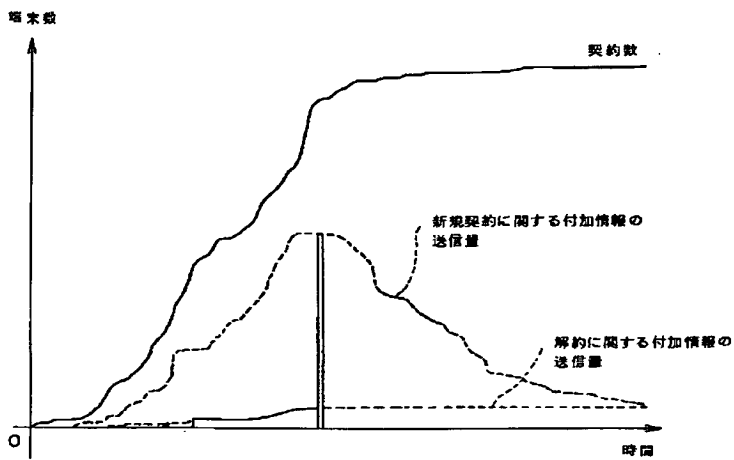
【図35】



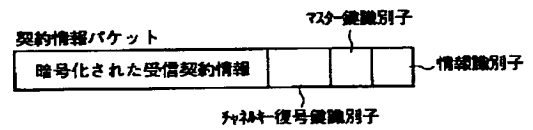
【図14】



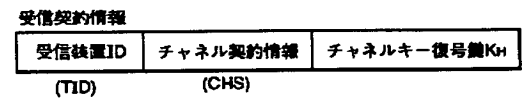
【図19】



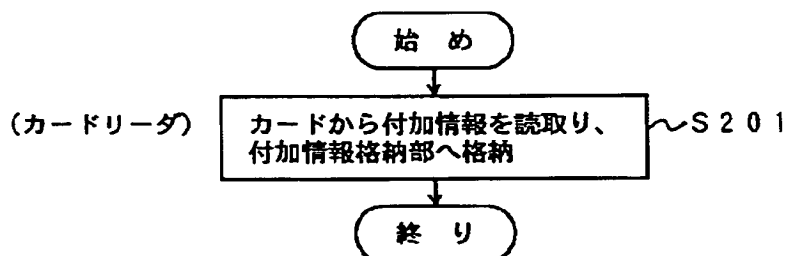
【図37】



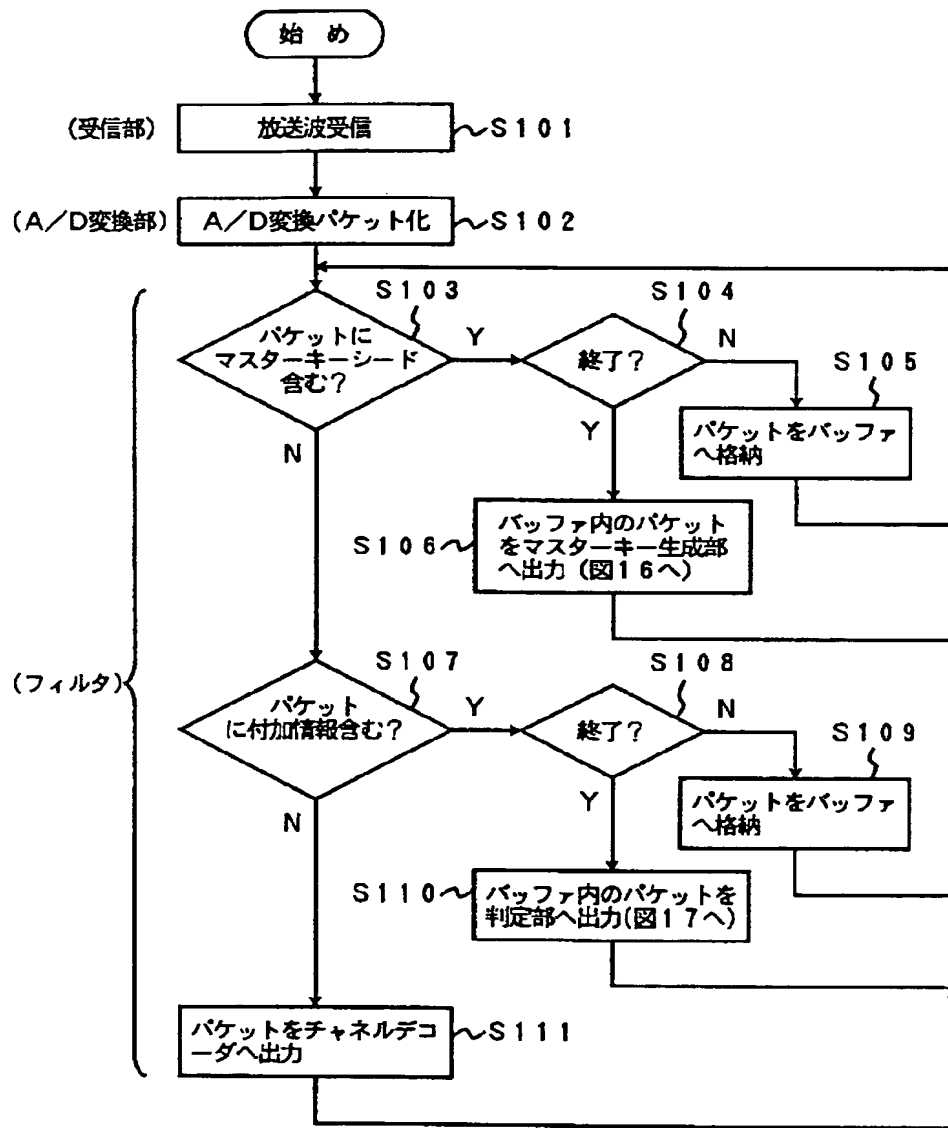
【図38】



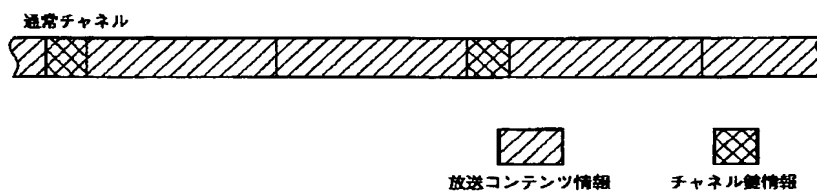
【図28】



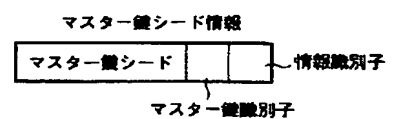
【図15】



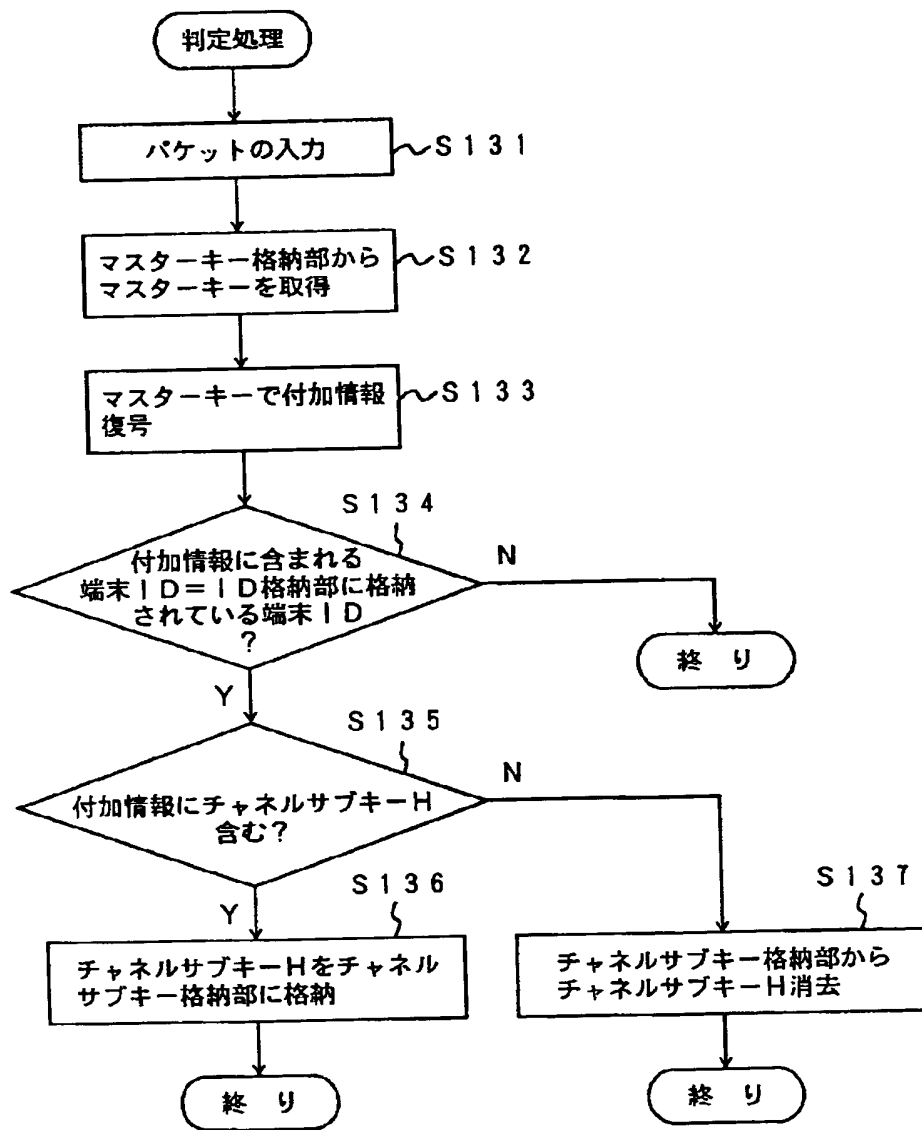
【図33】



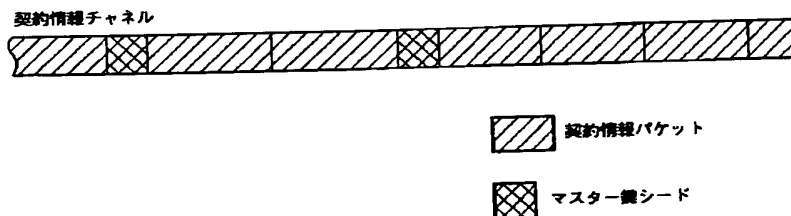
【図39】



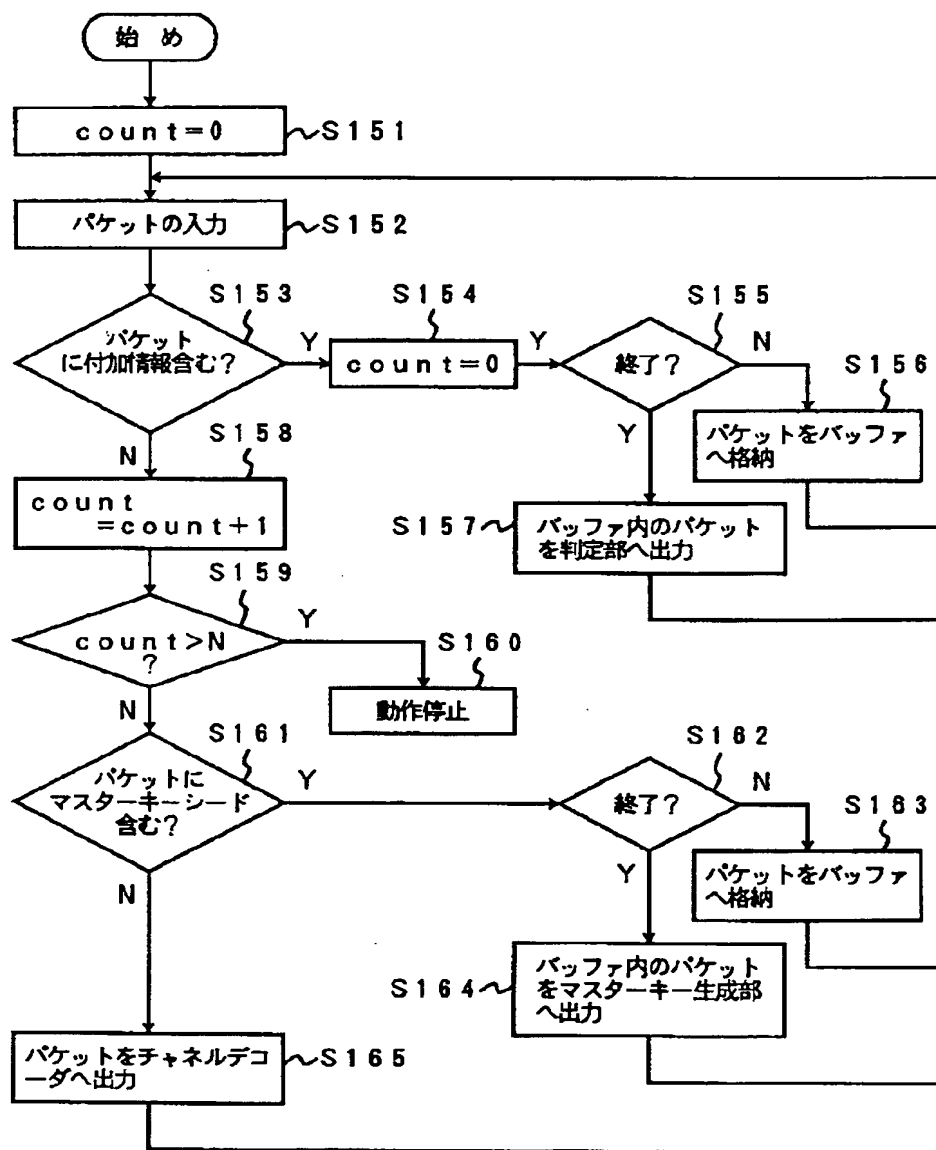
【図17】



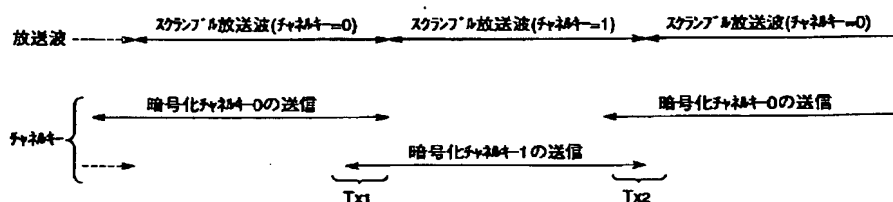
【図36】



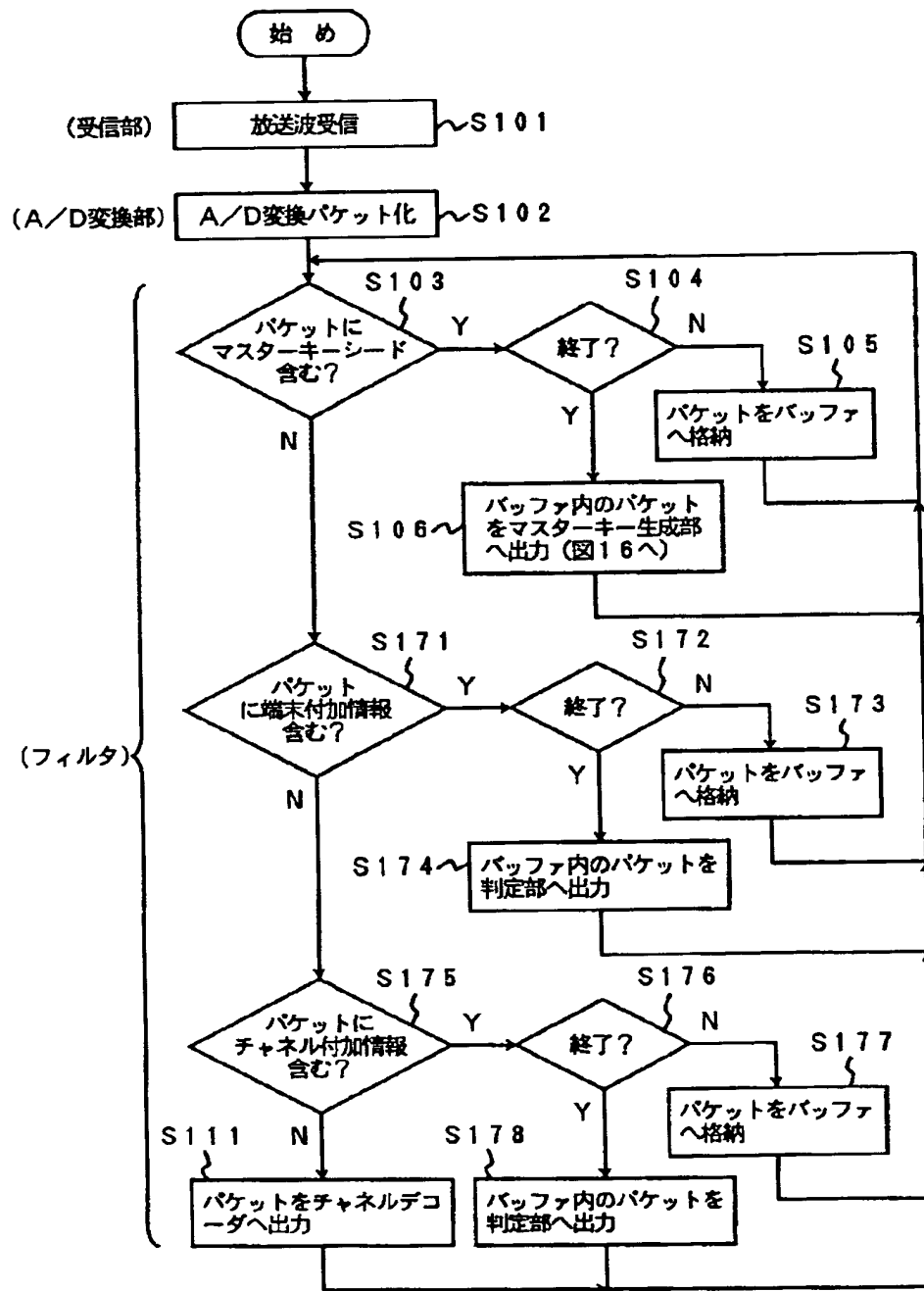
【図20】



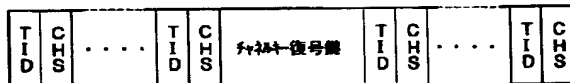
【図40】



【図21】

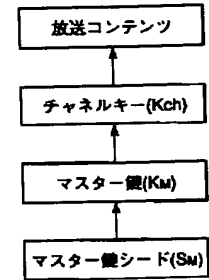


【図49】

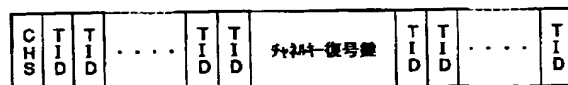


TID: 受信装置ID
CHS: チャンネル契約情報

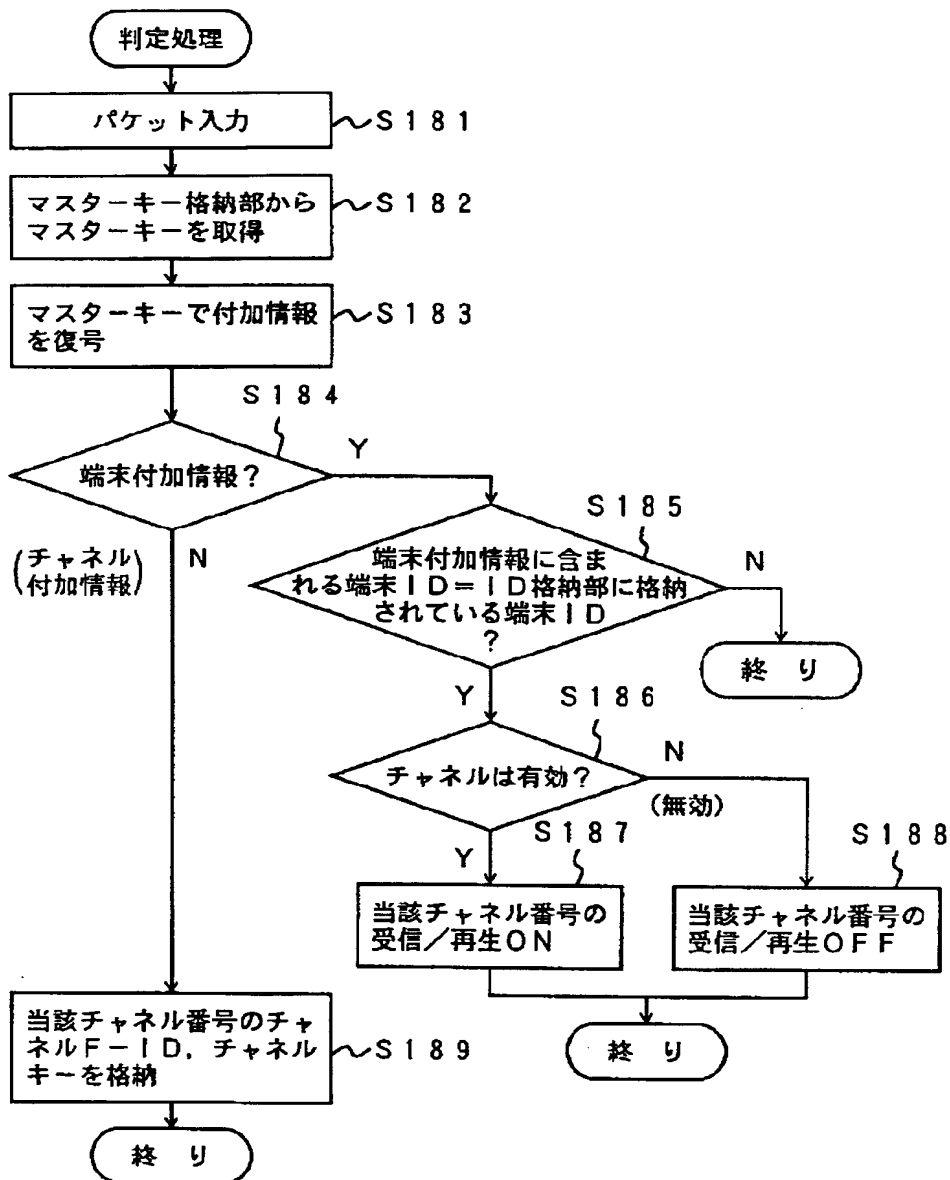
【図52】



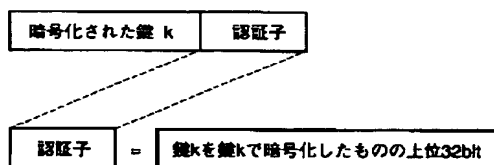
【図50】



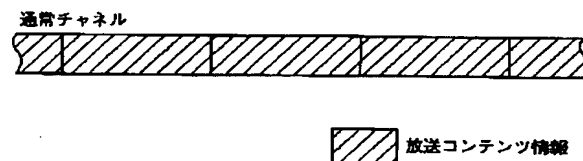
【図22】



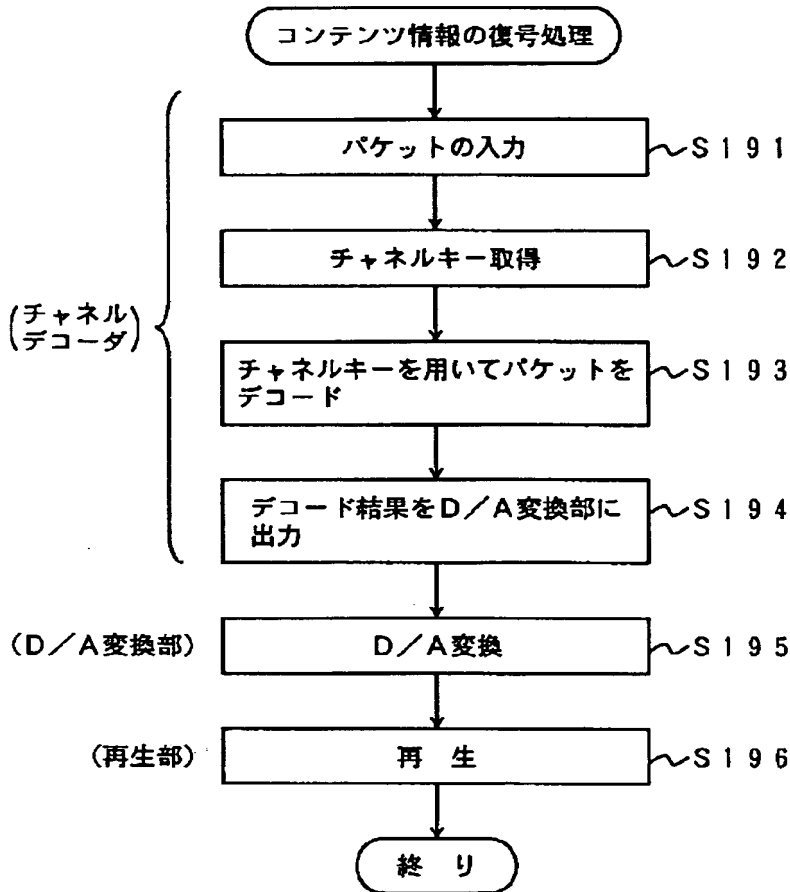
【図46】



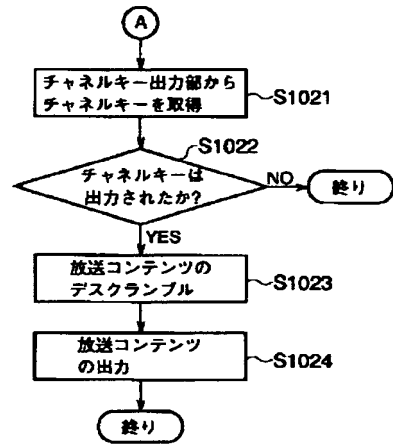
【図53】



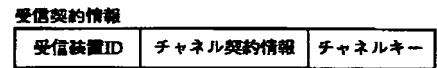
【図23】



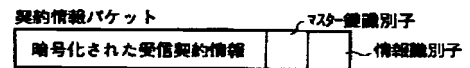
【図43】



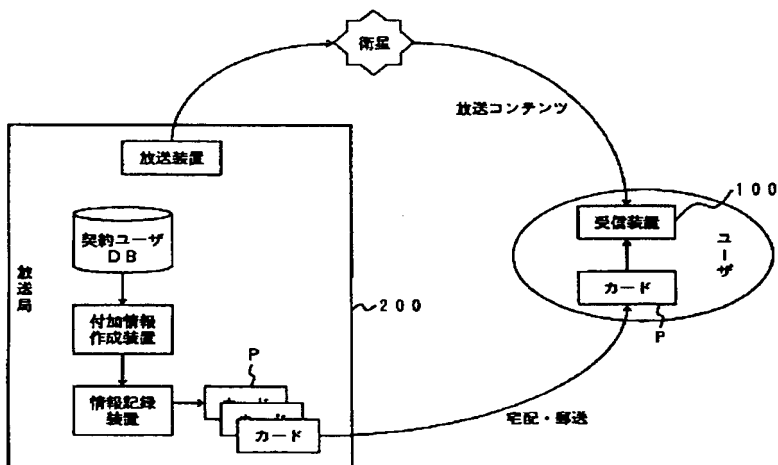
【図55】



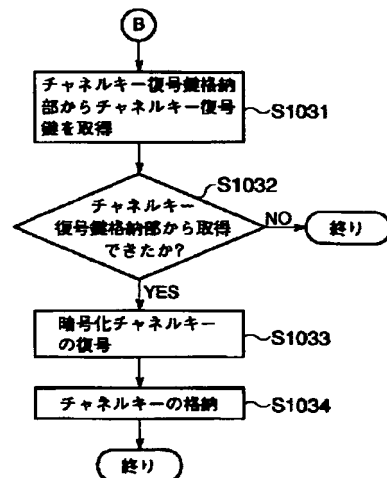
【図56】



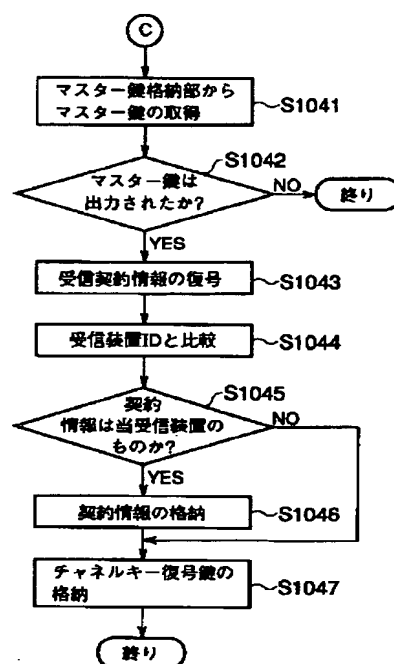
【図24】



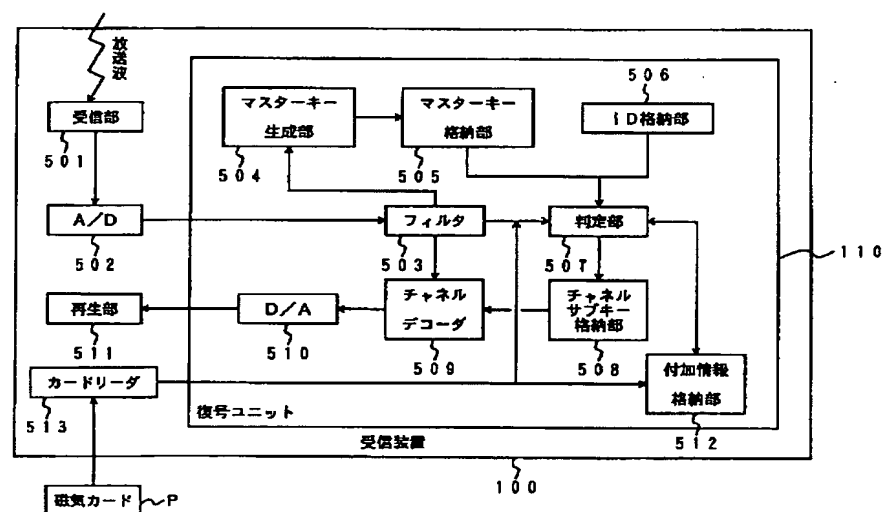
【図44】



【图 45】



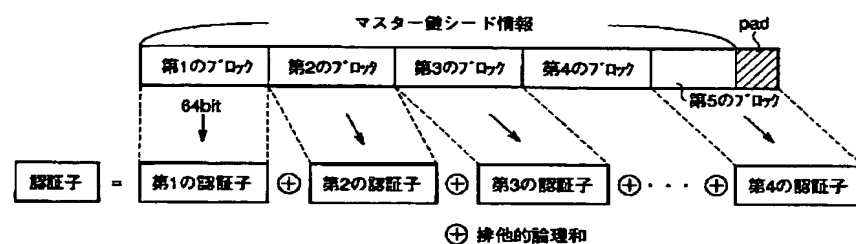
【圖 26】



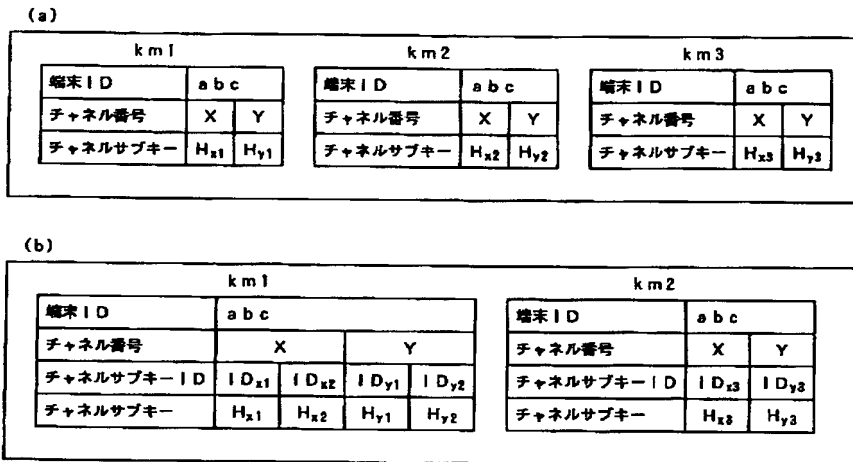
【图 59】

種別子		
種別子	種別子	種別子
チャネルキー	0	1
チャネルキー	1	
チャネルキー	0	2
チャネルキー	1	
チャネルキー	0	3
チャネルキー	1	
...		
...		
...		
チャネルキー	0	29
チャネルキー	1	
チャネルキー	0	30
チャネルキー	1	

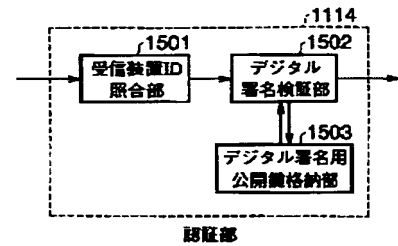
【圖 47】



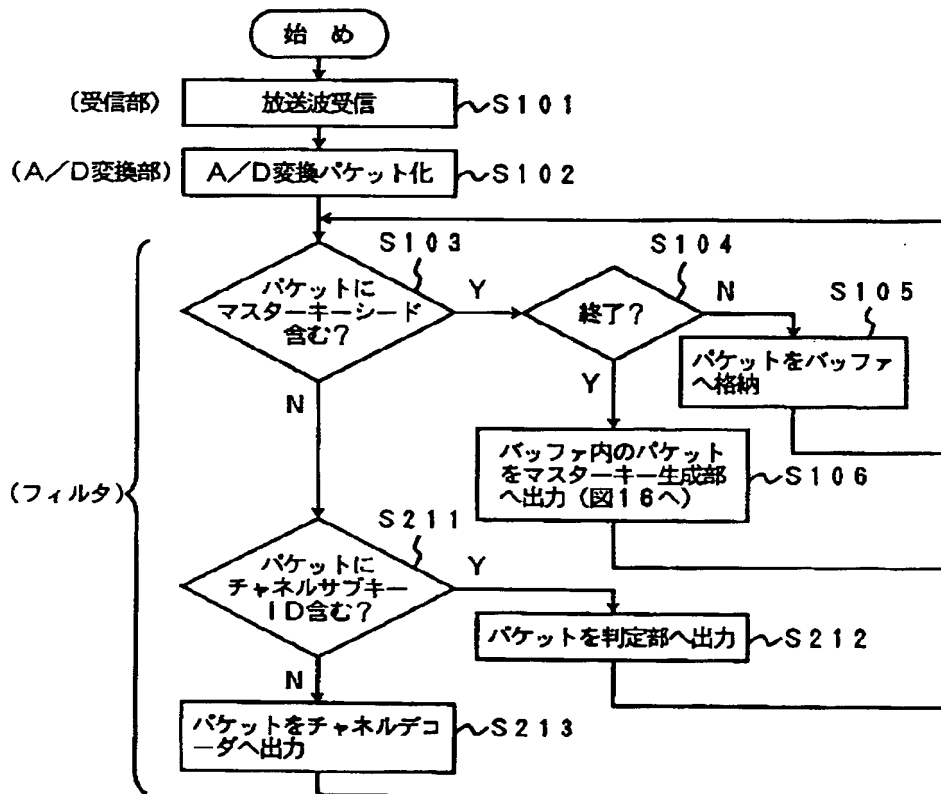
【図27】



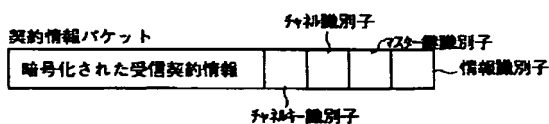
【図68】



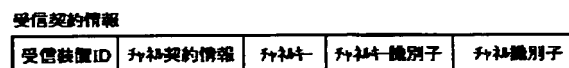
【図29】



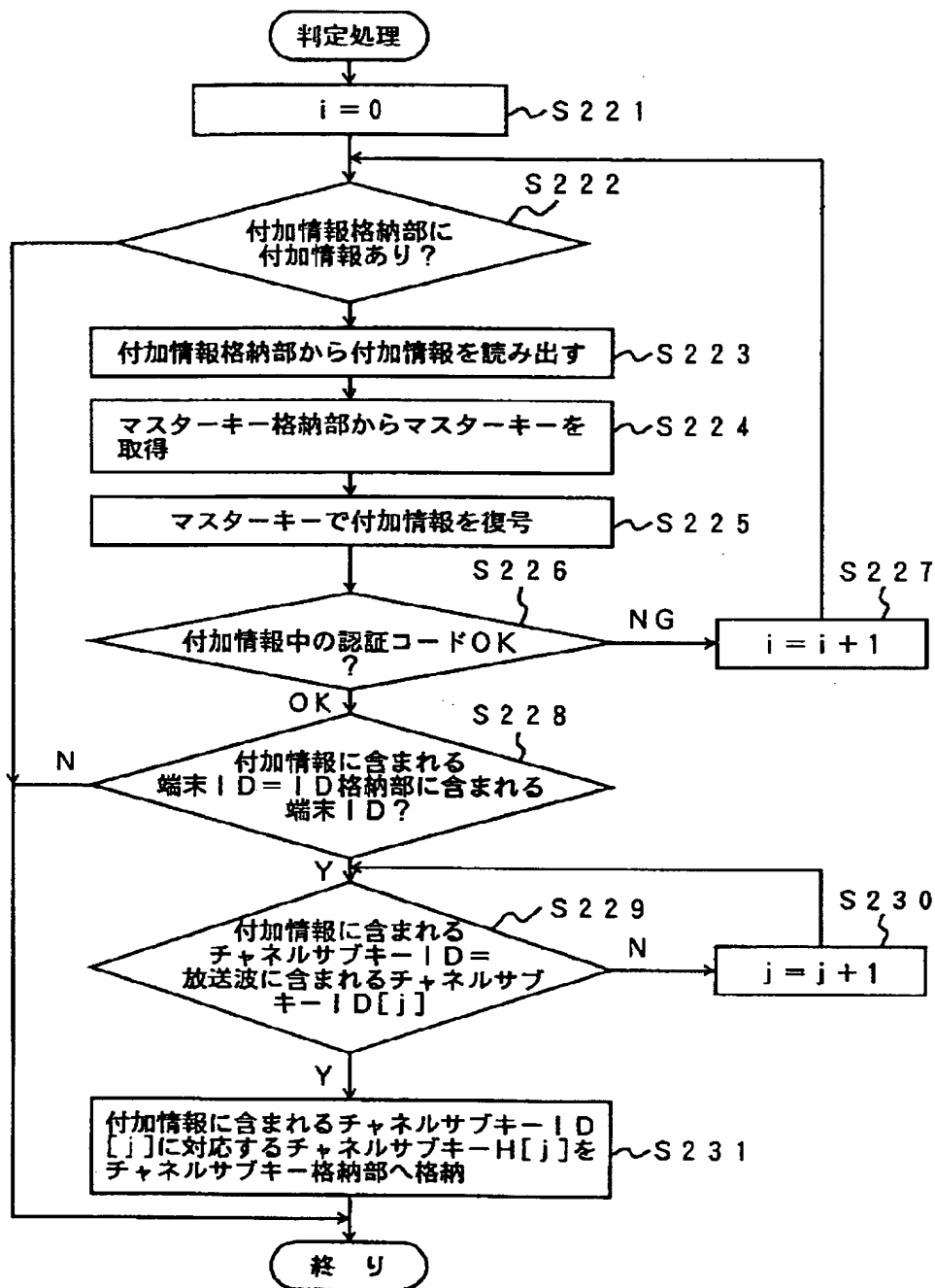
【図54】



【図57】



【図30】



【図58】

受信契約情報

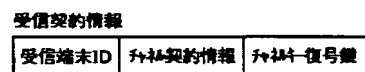
受信装置ID	付加契約情報	付加ID-0	付加ID-1	付加識別子
--------	--------	--------	--------	-------

【図64】

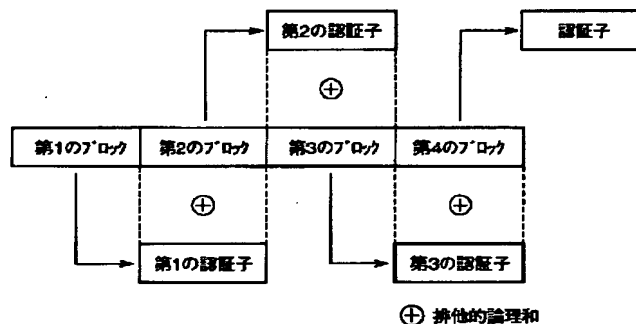
契約情報バケット

暗号化された 受信契約情報	認証情報	付加ID-復号 識別子	マスター鍵 識別子	情報識別子
------------------	------	----------------	--------------	-------

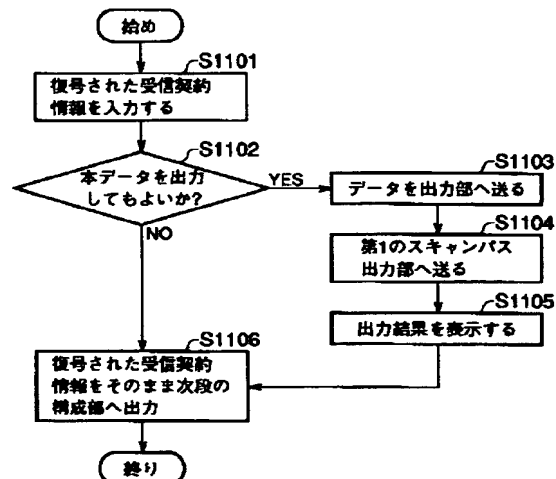
【图 7 4】



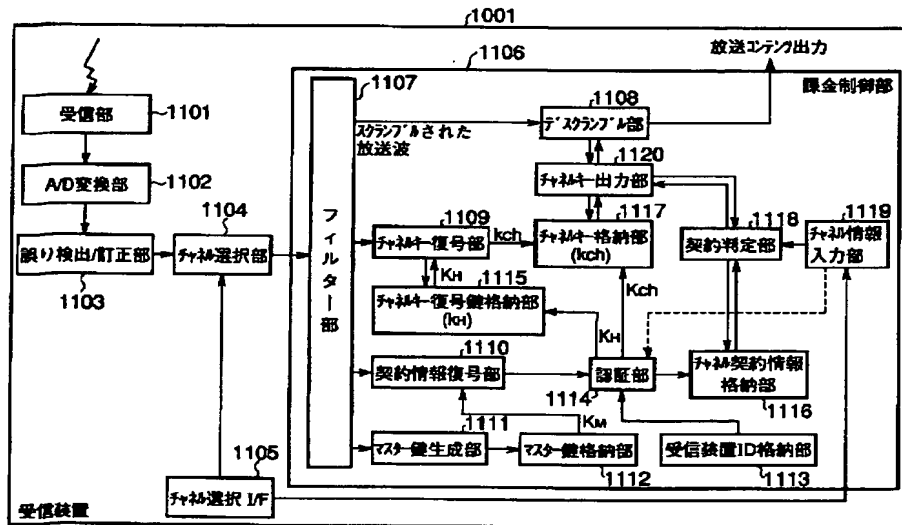
【图48】



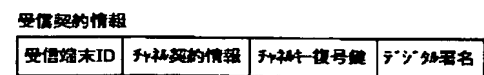
【图 6 3】



【図60】

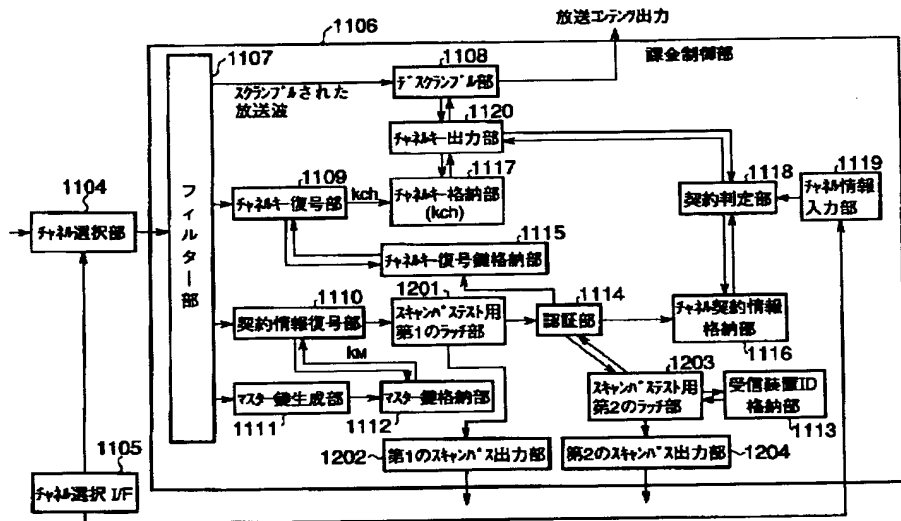


【図 69】

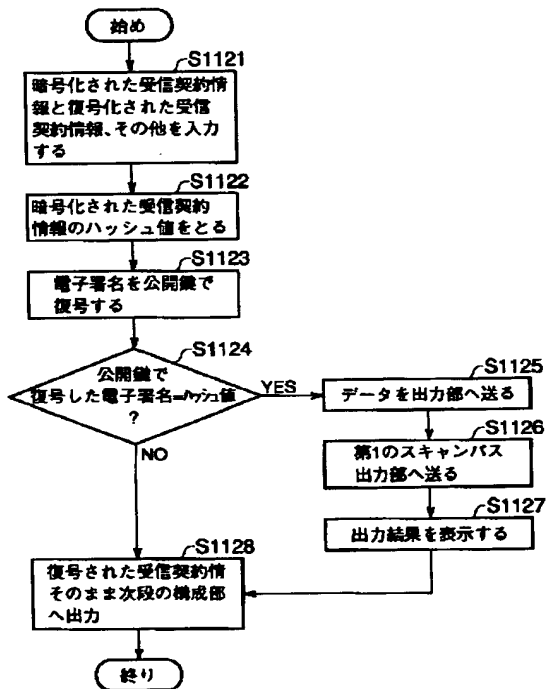


受信端末ID	升社契的情報	升社契復号鍵	証証子
--------	--------	--------	-----

【圖 6 1】



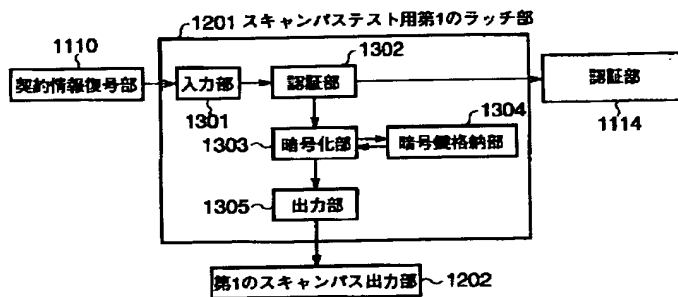
【图 65】



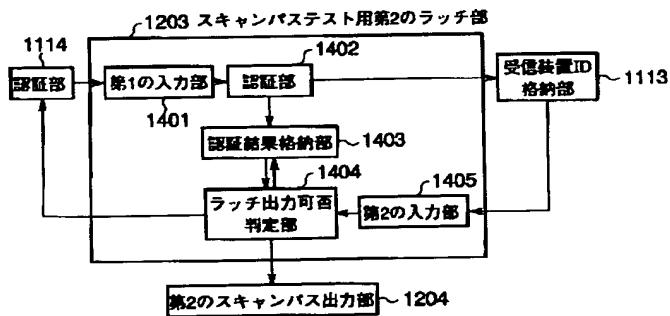
【図76】

受信契約情報				
受信端末ID	契約情報	契約番号	調子	署名

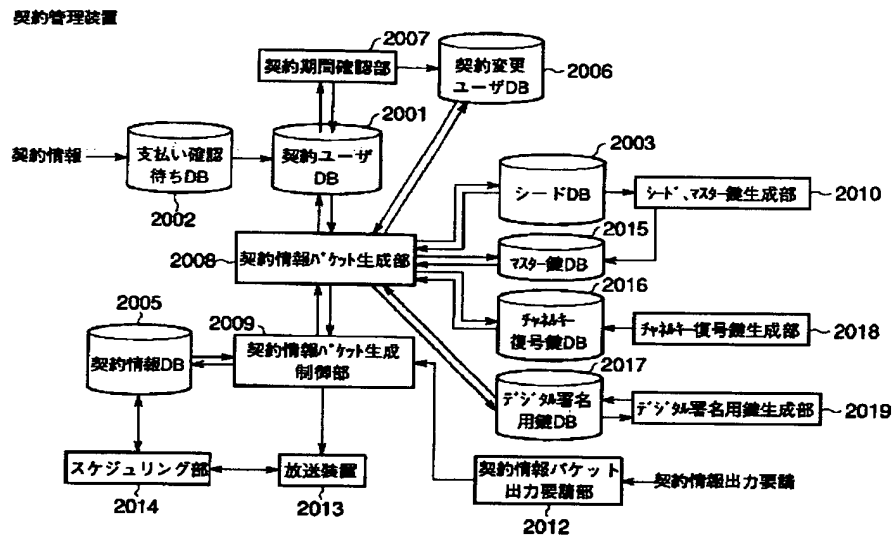
【图 6 6】



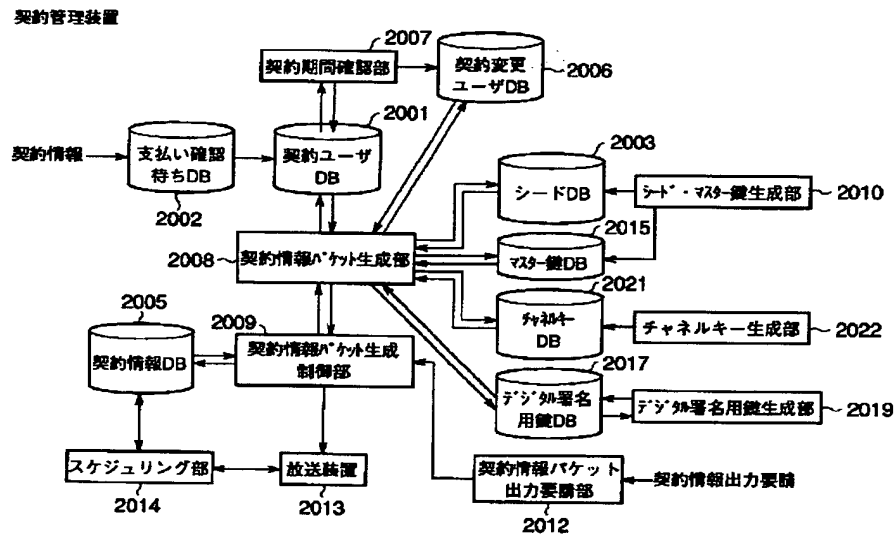
【图67】



【図70】



【図71】



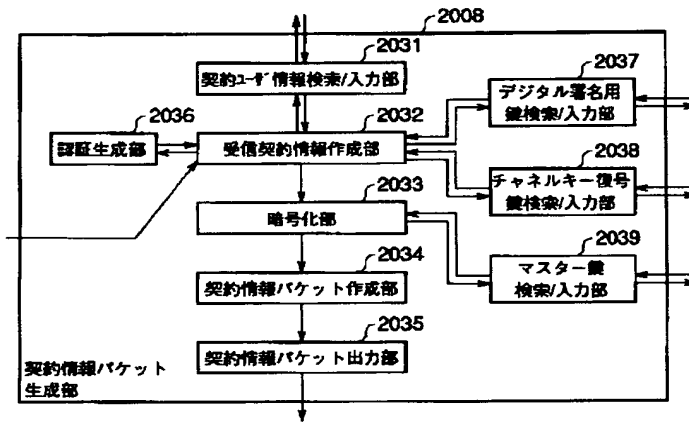
【図77】

TID	CHS	...	TID	CHS	チャンネルキー復号鍵	TID	CHS	...	TID	CHS	認証子	デジタル署名
-----	-----	-----	-----	-----	------------	-----	-----	-----	-----	-----	-----	--------

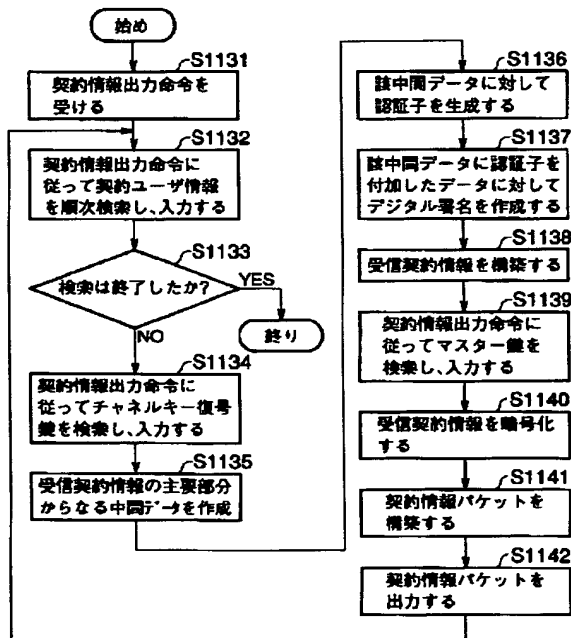
【図78】

CHS	TID	...	TID	TID	チャンネルキー復号鍵	TID	...	TID	認証子	デジタル署名
-----	-----	-----	-----	-----	------------	-----	-----	-----	-----	--------

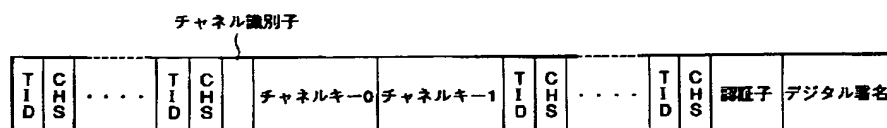
【図72】



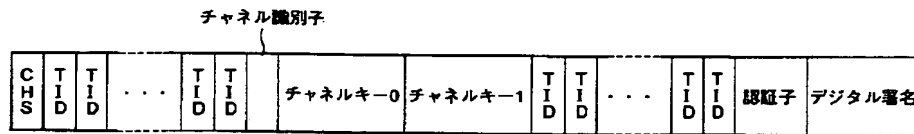
【図73】



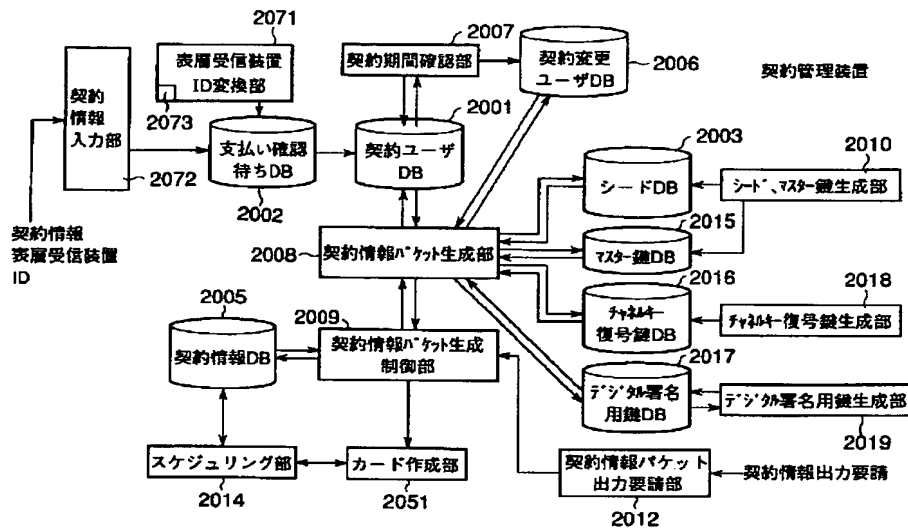
【図79】



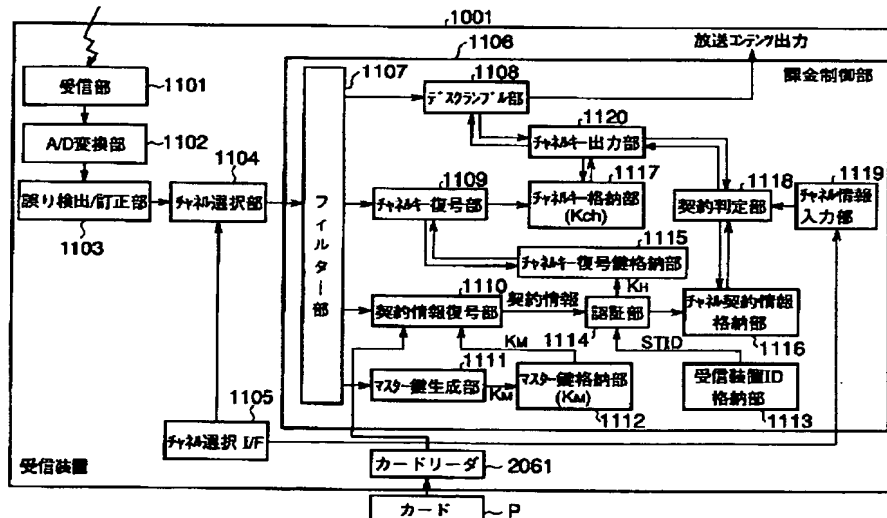
【図 8 1】



【図 8 2】



【圖 8 2】



フロントページの続き

(72)発明者 遠藤 直樹
東京都府中市東芝町 1 番地 株式会社東芝
府中工場内

【公報種別】 特許法第 17 条の 2 の規定による補正の掲載
 【部門区分】 第 7 部門第 3 区分
 【発行日】 平成 16 年 10 月 14 日 (2004.10.14)

【公開番号】 特開平 11-243536
 【公開日】 平成 11 年 9 月 7 日 (1999.9.7)
 【出願番号】 特願平 10-228287
 【国際特許分類第 7 版】

H 0 4 N 7/16
 H 0 4 H 1/00
 H 0 4 L 9/08
 H 0 4 L 9/32

【F I】

H 0 4 N 7/16 Z
 H 0 4 H 1/00 F
 H 0 4 L 9/00 6 0 1 A
 H 0 4 L 9/00 6 7 1

【手続補正書】
 【提出日】 平成 15 年 9 月 30 日 (2003.9.30)
 【手続補正 1】
 【補正対象書類名】 明細書
 【補正対象項目名】 特許請求の範囲
 【補正方法】 変更
 【補正の内容】
 【特許請求の範囲】
 【請求項 1】

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき、放送配信される暗号化コンテンツ情報を復号する放送受信装置において、
 複数の放送受信装置に共通のマスター鍵と本放送受信装置に一意に設定された識別情報とを格納する格納手段と、
 少なくとも前記契約情報と該契約情報に対応した識別情報と、前記暗号化されたコンテンツを復号するためのチャンネルキーとを含む暗号化された受信契約情報を受信する第 1 の受信手段と、
 前記第 1 の受信手段で受信した暗号化された受信契約情報を、前記マスター鍵を利用し、該暗号化された受信契約情報を順次復号する受信契約情報復号手段と、
 前記受信契約情報復号手段で復号した受信契約情報のうち、本放送受信装置の有する識別情報に一致する識別情報に対応付けられた契約情報を取得する契約情報取得手段と、
 前記契約情報取得手段で取得した該契約情報に基づき、前記コンテンツ情報の視聴の可否を判定する判定手段と、
 前記判定手段で視聴可と判定された際に、前記受信契約情報復号手段で復号されたチャンネルキーで暗号化されたコンテンツ情報を復号するコンテンツ復号手段とを備えたことを特徴とする放送受信装置。

【請求項 2】

前記受信契約情報は、少なくとも前記識別情報を含む第 1 の受信契約情報と少なくとも前記チャンネルキーを含む第 2 の受信契約情報とからなり、前記受信手段で前記第 1 の受信契約情報と前記第 2 の受信契約情報とが受信されたときに、前記コンテンツ復号手段で前記暗号化されたコンテンツ情報を復号することを特徴とする請求項 1 記載の放送受信装置。

【請求項 3】

前記受信契約情報には、前記チャンネルキーの一部を含み、前記受信手段は、前記チャンネル

キーの他の一部を別途受信することを特徴とする請求項 1 記載の放送受信装置。

【請求項 4】

暗号化されたコンテンツ情報を含む通常放送波を受信する第 2 の受信手段をさらに具備し、

前記第 1 の受信手段は、暗号化された前記チャンネルキーを復号するためのチャンネルキー復号鍵をさらに含む前記暗号化された前記受信契約情報を含む契約放送波を受信し、

前記第 1 の受信手段で受信した前記暗号化された受信契約情報を前記マスター鍵に基づいて復号して前記チャンネルキー復号鍵を取得し、その取得したチャンネルキー復号鍵を用いて、前記暗号化チャンネルキーを復号することによってチャンネルキーを取得し、前記取得した契約情報に基づき、前記コンテンツ情報の視聴の可否を判定することを特徴とする請求項 1 記載の放送受信装置。

【請求項 5】

暗号化されたコンテンツ情報と前記チャンネルキーの一部を含む通常放送波を受信する第 2 の受信手段をさらに具備し、

前記第 1 の受信手段は、前記チャンネルキーの他の一部を含む前記暗号化された受信契約情報を含む契約放送波を受信し、

前記第 1 の受信手段で受信した前記暗号化された受信契約情報を前記マスター鍵に基づいて復号して前記チャンネルキーの他の一部と前記契約情報を取得し、前記第 2 の受信手段で受信したチャンネルキーの一部と前記取得したチャンネルキーの他の一部とからチャンネルキーを再生し、前記取得した契約情報に基づき、前記コンテンツ情報の視聴の可否を判定することを特徴とする請求項 1 記載の放送受信装置。

【請求項 6】

暗号化されたコンテンツ情報を復号するための内容の正確性が要求される必須情報の誤受信検出のために、それぞれの必須情報に認証子が付加されたデータを受信し、前記認証子とそれが付加された必須情報とを照合し、照合に失敗した場合は当該必須情報を無効にすることを特徴とする請求項 1 記載の放送受信装置。

【請求項 7】

前記受信契約情報に含まれるデジタル署名を検証し、検証により正当性の確認されたデジタル署名を持つ受信契約情報に含まれる契約情報のみを受理することを特徴とする請求項 1 記載の放送受信装置。

【請求項 8】

内部データをテスト出力するためのテスト制御部を具備し、このテスト制御部は、前記受信契約情報に付加されたテスト用である旨の識別子を確認することにより、あるいは、該受信契約情報に付加されたデジタル署名の正当性を確認することにより、前記内部データをテスト出力するか否かを制御することを特徴とする請求項 1 記載の放送受信装置。

【請求項 9】

暗号化された受信契約情報を記録したカード型記録媒体から該暗号化された受信契約情報を読み出して本放送受信装置に受信させるカードリーダーを具備したことを特徴とする請求項 1 記載の放送受信装置。

【請求項 10】

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき暗号化されたコンテンツ情報を復号する複数の放送受信装置を管理する契約管理装置であって、少なくとも前記複数の放送受信装置のそれぞれに一意に設定された識別情報と該識別情報に対応し前記放送受信装置ごとの前記契約情報とを含む受信契約情報を前記複数の放送受信装置に共通のマスター鍵に基づいて暗号化して配信する手段と、前記暗号化されたコンテンツ情報を復号するためのチャンネルキーを配信する手段と、を具備したことを特徴とする契約管理装置。

【請求項 11】

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき暗号化されたコン

コンテンツ情報を復号する複数の放送受信装置を管理する契約管理装置であって、少なくとも前記複数の放送受信装置のそれぞれに一意に設定された識別情報と該識別情報に対応し、前記放送受信装置ごとの前記契約情報と前記暗号化されたコンテンツ情報を復号するための暗号化されたチャンネルキーを復号するためのチャンネルキー復号鍵とを含む受信契約情報を前記複数の放送受信装置に共通のマスター鍵に基づいて暗号化して配信する手段を具備したことを特徴とする契約管理装置。

【請求項 1 2】

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき暗号化されたコンテンツ情報を復号する複数の放送受信装置を管理する契約管理装置であって、少なくとも前記複数の放送受信装置のそれぞれに一意に設定された識別情報と該識別情報に対応し、前記放送受信装置ごとの前記契約情報として前記暗号化されたコンテンツ情報を復号するためのチャンネルキーの一部とを含む受信契約情報を前記複数の放送受信装置に共通のマスター鍵に基づいて暗号化して配信する手段と、前記チャンネルキーの他の一部を配信する手段と、を具備したことを特徴とする契約管理装置。

【請求項 1 3】

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき暗号化されたコンテンツ情報を復号する複数の放送受信装置を管理する契約管理装置であって、少なくとも前記複数の放送受信装置のそれぞれに一意に設定された識別情報と、該識別情報に対応し、前記放送受信装置ごとの前記契約情報と、前記暗号化されたコンテンツ情報を復号するためのチャンネルキーとを含む受信契約情報を前記複数の放送受信装置に共通のマスター鍵に基づいて暗号化して放送配信する手段を具備したことを特徴とする契約管理装置。

【請求項 1 4】

カード型記録媒体に前記暗号化された受信契約情報を記録する記録手段を具備したことを特徴とする請求項 1 0 ～請求項 1 3 のいずれか 1 つに記載の契約管理装置。

【請求項 1 5】

契約に変化の生じた契約者の受信契約情報を選択的に送信することを特徴とする請求項 1 0 ～請求項 1 3 のいずれか 1 つに記載の契約管理装置。

【請求項 1 6】

前記受信契約情報に含まれる情報の種別に応じた識別子に基づき、該受信契約情報に対する処理形態を切り替えることを特徴とする請求項 1 記載の放送受信装置。

【請求項 1 7】

前記受信契約情報を送信すべき契約者の数に応じて、受信契約情報の送信形態を切り替えることを特徴とする請求項 1 0 ～請求項 1 3 のいずれか 1 つに記載の契約管理装置。

【手続補正 2】

【補正対象書類名】 明細書

【補正対象項目名】 0 0 1 0

【補正方法】 変更

【補正の内容】

【0 0 1 0】

【課題を解決するための手段】

(1) 暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき、放送配信される暗号化コンテンツ情報を復号する放送受信装置において、複数の放送受信装置に共通のマスター鍵と本放送受信装置に固有に設定された受信装置 ID を持ち、少なくとも前記契約情報と該契約情報に対応した受信装置 ID を含む暗号化された受信契約情報を受信したとき、前記マスター鍵を用いて、該暗号化された受信契約情報を順次復号し、該復号された受信契約情報のうち、本放送受信装置の有する受信装置 ID に一致する受信装置 ID に対応付けられた契約情報を選択して取得し、その取得した契約情報に基づき、暗号化された情報コンテンツを復号するチャンネルキーを暗号化されたコンテンツ情報を復号する

ための復号部に送るか否か制御することを特徴とする。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正の内容】

【0012】

(2) 第2の実施形態（チャンネルキーは、受信契約情報とは別途に配布）
請求項1記載の放送受信装置において、前記チャンネルキーは別途受信し、前記受信契約情報を受信しない限り、前記チャンネルキーは前記復号部に送られることがないように制御することを特徴とする。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【0013】

(3) 第3の実施形態（受信契約情報にチャンネルキー復号鍵が含まれる）
上記(1)記載の放送受信装置において、暗号化された前記チャンネルキーを別途受信し、この暗号化されたチャンネルキーを復号するチャンネルキー復号鍵を含む前記受信契約情報を受信しない限り、前記チャンネルキーが復号されないよう制御することを特徴とする。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

【補正の内容】

【0014】

(4) 第1の実施形態（受信契約情報にチャンネルキーの一部が含まれる）
上記(1)記載の放送受信装置において、前記チャンネルキーの一部は別途受信され、前記チャンネルキーの他の一部を含む前記受信契約情報を受信しない限り、前記チャンネルキーが得られないように制御することを特徴とする。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】変更

【補正の内容】

【0015】

(5) 第4の実施形態（受信契約情報にチャンネルキーが含まれる）
上記(1)記載の放送受信装置において、前記チャンネルキーは、前記受信契約情報に含まれて受信され、前記受信契約情報を受信しない限り、前記チャンネルキーが得られないものであることを特徴とする。

(6) 第2の実施形態（チャンネルキーは、受信契約情報とは別途に配布）

上記(1)記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第1の受信手段と、前記暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段と、を具備し、前記マスター鍵を用いて、前記第1もしくは第2の受信手段で受信した暗号化されたチャンネルキーを復号してチャンネルキーを取得するとともに、前記第2の受信手段で受信した暗号化された受信契約情報を復号して前記契約情報を取得し、その取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【手続補正 7】

【補正対象書類名】明細書
【補正対象項目名】0016
【補正方法】変更
【補正の内容】
【0016】

(7) 第3の実施形態（受信契約情報にチャンネルキー復号鍵が含まれる）

上記(1)記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第1の受信手段と、前記暗号化されたチャンネルキーを復号するためのチャンネルキー復号鍵を含む暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段と、を具備し、前記マスター鍵を用いて、前記第2の受信手段で受信した暗号化された受信契約情報を復号して前記チャンネルキー復号鍵を取得し、その取得したチャンネルキー復号鍵を用いて、前記第1もしくは第2の受信手段で受信した暗号化チャンネルキーを復号することによってチャンネルキーを取得し、前記取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【手続補正8】
【補正対象書類名】明細書
【補正対象項目名】0017
【補正方法】変更
【補正の内容】
【0017】

(8) 第1の実施形態（受信契約情報にチャンネルキーの一部が含まれる）

上記(1)記載の放送受信装置において、暗号化された放送コンテンツ情報と前記チャンネルキーの一部を含む通常放送波を受信する第1の受信手段と、前記チャンネルキーの他の一部を含む暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段を具備し、前記マスター鍵を用いて、前記第2の受信手段で受信した暗号化された受信契約情報を復号して前記チャンネルキーの他の一部と前記契約情報を取得し、前記第1の受信手段で受信したチャンネルキーの一部と前記取得したチャンネルキーの他の一部とからチャンネルキーを再生し、前記取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【手続補正9】
【補正対象書類名】明細書
【補正対象項目名】0018
【補正方法】変更
【補正の内容】
【0018】

(9) 第4の実施形態（受信契約情報にチャンネルキーが含まれる）

上記(1)記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第1の受信手段と、前記チャンネルキーを含む暗号化された受信契約情報を含む契約放送波を受信する第2の受信手段と、を具備し、前記マスター鍵を用いて、前記第2の受信手段で受信した暗号化された受信契約情報を復号して該受信契約情報に含まれる契約情報とチャンネルキーを取得し、その取得した契約情報に基づき、前記チャンネルキーを暗号化されたコンテンツ情報の復号部に送るか否か制御することを特徴とする。

(10) 上記(1)～(9)記載の放送受信装置において、チャンネルキー、マスター鍵の少なくとも一方が変更されることを特徴とする。

【手続補正10】
【補正対象書類名】明細書
【補正対象項目名】0019
【補正方法】変更
【補正の内容】

【0019】

鍵情報に有効期間が定められていることにより、契約期間の管理（契約期間の開始、終了、継続等）が容易に行える。また、コンテンツの不正視聴防止等のセキュリティの向上が図れる。

(11) 上記(1)、(3)、(7)記載の放送受信装置において、チャンネルキーおよびチャンネルキー復号鍵およびマスター鍵のうちの少なくとも1つが変更されることを特徴とする。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0020

【補正方法】変更

【補正の内容】

【0020】

鍵情報に有効期間が定められていることにより、契約期間の管理（契約期間の開始、終了、継続等）が容易に行える。また、コンテンツの不正視聴防止等のセキュリティの向上が図れる。

(12) 上記(1)～(9)記載の放送受信装置において、チャンネルキー、マスター鍵の少なくとも一方が変更され、チャンネルキー、マスター鍵のそれぞれは、同時に最大2つの鍵を保持することを特徴とする。

(13) 上記(1)～(9)記載の放送受信装置において、チャンネルキー、マスター鍵の少なくとも一方が変更され、チャンネルキー、マスター鍵のそれぞれにおいて同時に最大2つの鍵を保持し、鍵変更の際には古い方を更新することを特徴とする。

(14) 上記(1)、(3)、(7)記載の放送受信装置において、チャンネルキーおよびチャンネルキー復号鍵およびマスター鍵のうちの少なくとも一つが変更され、チャンネルキー、チャンネルキー復号鍵、マスター鍵のそれぞれは、同時に最大2つの鍵を保持することを特徴とする。

(15) 上記(1)、(3)、(7)記載の放送受信装置において、チャンネルキーおよびチャンネルキー復号鍵およびマスター鍵のうちの少なくとも1つが変更され、チャンネルキー、チャンネルキー復号鍵、マスター鍵のそれぞれは、同時に最大2つの鍵を保持し、鍵変更の際には古い方を更新することを特徴とする。

(16) 上記(1)～(9)記載の放送受信装置において、チャンネルキーは、チャンネル毎に同時に最大2つ保持することを特徴とする。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0021

【補正方法】変更

【補正の内容】

【0021】

チャンネルキーをチャンネル毎に最大2つ保持することにより、チャンネル切替時であっても（切替元にチャンネルの受信契約を行っていれば）、保持している当該チャンネルのチャンネルキーを暗号化されたコンテンツ情報の復号部に即時的に送ることでチャンネル切替の受信状態を良好にできる。

(17) 上記(1)記載の放送受信装置において、暗号化されたコンテンツ情報を復号するための内容の正確性が要求される必須情報（例えば、チャンネルキー等の鍵情報、受信契約情報）の誤受信検出のために、それぞれの必須情報に認証子が付加されたデータを受信し、前記認証子とそれが付加された必須情報とを照合し、照合に失敗した場合は当該必須情報を無効にすることを特徴とする。

(18) 上記(17)記載の放送受信装置において、暗号化された必須情報の認証子は、該必須情報を該必須情報で暗号化したもの、あるいは、その一部であることを特徴とする。

(19) 上記(17)記載の放送受信装置において、暗号化された必須情報の認証子は、該必須情報を該必須情報で暗号化したもの、あるいは、前記暗号化された必須情報を該必須情報で再暗号化したもの、あるいは、数回再暗号化した情報のうち全部あるいは一部であることを特徴とする。

(20) 上記(17)記載の放送受信装置において、暗号化されていない必須情報（例えば、マスター鍵シード）の認証子は、該必須情報を必要があればブロック分割し、それぞれのブロックの情報を鍵として当該情報を暗号化したもの、あるいは、それをさらに圧縮したものを用いることを特徴とする。

(21) 上記(1)記載の放送受信装置において、前記受信契約情報に含まれるデジタル署名を検証し、検証により正当性の確認されたデジタル署名を持つ受信契約情報に含まれる契約情報のみを受理することを特徴とする。

(22) 上記(21)記載の放送受信装置において、受信契約情報に当該放送受信装置に対する契約情報が含まれた時のみ、受信契約情報に含まれるデジタル署名を検証することを特徴とする。

(23) 上記(21)記載の放送受信装置において、デジタル署名検証用の公開鍵を変更することを特徴とする。

(24) 上記(1)記載の放送受信装置において、内部データ（復号された受信契約情報、放送受信装置内の受信装置ID格納部に格納されている受信装置ID）をテスト出力するためのテスト制御部（スキャンパステスト用ラッチ部）を具備し、このテスト制御部は、前記受信契約情報に付加されたテスト用である旨の識別子を確認することにより、あるいは、該受信契約情報に付加されたデジタル署名の正当性を確認することにより、前記内部データをテスト出力するか否かを制御することを特徴とする。

(25) 上記(24)記載の放送受信装置において、前記テスト制御部は、暗号化された内部データを出力することを特徴とする。

(26) 上記(1)記載の放送受信装置において、暗号化された受信契約情報を記録したカード型記録媒体から該暗号化された受信契約情報を読み出して本放送受信装置に受信させるカードリーダーを具備したことを特徴とする。

(27) 上記(26)記載の放送受信装置において、前記カードリーダーは、有効期間毎に複数の契約情報が記録された磁気カードから、前記複数の契約情報を読み出し、有効期間に応じてそれらの複数の契約情報を使い分けることを特徴とする。

(28) 契約管理装置

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき放送配信される暗号化コンテンツ情報を復号することにより該コンテンツ情報を受信する複数の放送受信装置を管理する契約管理装置において、少なくとも放送受信装置毎個別に設定された受信装置IDと該受信装置IDに対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0022

【補正方法】変更

【補正の内容】

【0022】

本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(29) 第2の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーは暗号化されたコンテンツ情報を復号するための復号部に送られることがないように制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定さ

れた受信装置IDと該受信装置IDに対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、前記チャンネルキーは前記受信契約情報とは別途配信することを特徴とする。

【手続補正14】

【補正対象書類名】明細書

【補正対象項目名】0023

【補正方法】変更

【補正の内容】

【0023】

本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(30) 第3の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するための暗号化されたチャンネルキーが復号されないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置IDと該受信装置IDに対応した契約情報と前記暗号化されたチャンネルキーを復号するためのチャンネルキー復号鍵とを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【手続補正15】

【補正対象書類名】明細書

【補正対象項目名】0024

【補正方法】変更

【補正の内容】

【0024】

本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(31) 第1の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャンネルキーが得られないように制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置IDと、該受信装置IDに対応した契約情報として前記チャンネルキーの一部を含むものとを包含する受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、前記チャンネルキーの他の一部を別途送信することを特徴とする。

【手続補正16】

【補正対象書類名】明細書

【補正対象項目名】0025

【補正方法】変更

【補正の内容】

【0025】

本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(32) 第4の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャンネルキーが得られないように、複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置IDと該受信装置IDに対応

した契約情報と前記チャンネルキーとを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【手続補正17】

【補正対象書類名】明細書

【補正対象項目名】0026

【補正方法】変更

【補正の内容】

【0026】

本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

(33) 上記(29)～(30)記載の契約管理装置において、チャンネルキーおよびマスター鍵のうち少なくとも1つが予め定められた期間で変更されることを特徴とする。

(34) 上記(29)～(32)記載の契約管理装置において、チャンネルキーおよびチャンネルキー復号鍵およびマスター鍵のうち少なくとも1つが予め定められた期間で変更されることを特徴とする。

(35) 上記(29)～(32)記載の契約管理装置において、前受信契約情報に対する認証子を受信契約情報に含めて送信することを特徴とする。

(36) 上記(29)～(32)記載の契約管理装置において、前記受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報に含まれる鍵情報で前記契約情報を暗号化したもの、もしくは、その一部を用いることを特徴とする。

(37) 上記(29)～(32)記載の契約管理装置において、受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報に含まれる鍵情報を該鍵情報で暗号化したもの、前記暗号化された鍵情報を鍵情報で再暗号化したもの、もしくは数回再暗号化した情報のうち全部もしくは一部を用いることを特徴とする。

(38) 上記(29)～(32)記載の契約管理装置において、受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報を必要があればブロック分割し、それぞれのブロックの情報を鍵として当該情報を暗号化し、必要があれば圧縮したものを用いることを特徴とする。

(39) 上記(29)～(32)記載の契約管理装置において、受信契約情報に該受信契約情報に対するデジタル署名を付加して送信することを特徴とする。

(40) 上記(29)～(32)記載の契約管理装置において、受信契約情報に該受信契約情報に対するデジタル署名を付加して送信し、デジタル署名検証用の公開鍵と作成用の秘密鍵のペアを生成する機構を具備し、一定期間で前記デジタル署名用の公開鍵と秘密鍵を変更すると共に、前記デジタル署名検証用の公開鍵を送信することを特徴とする。

(41) 上記(29)～(32)記載の契約管理装置において、カード型記録媒体に前記暗号化された受信契約情報を記録する記録手段を具備したことを特徴とする。

(42) 上記(29)～(32)記載の契約管理装置において、最近一定期間内に契約の変化の生じた(新規契約を含む)契約者の受信契約情報を選択的に送信することを特徴とする。

【手続補正18】

【補正対象書類名】明細書

【補正対象項目名】0027

【補正方法】変更

【補正の内容】

【0027】

契約の種類(例えば、契約変更、新規契約など)と契約後の経過期間によって、契約情報の放送頻度を変更するようにしてもよい。

(42-1) 上記(29)～(32)記載の契約管理装置において、契約の変化の生じた(新規契約を含む)時期により、受信契約情報の送信頻度を変化させることを特徴とする

- °
(43) 上記(1)～(9)、(17)、(21)、(24)、(26)記載の放送受信装置において、前記受信契約情報に含まれる情報の種別に応じた識別子(情報識別子)に基づき、該受信契約情報に対する処理形態を切り替えることを特徴とする。
(44) 上記(29)～(32)記載の契約管理装置において、前記受信契約情報を送信すべき契約者の数に応じて、受信契約情報の送信形態を切り替えることを特徴とする。

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE LEFT BLANK